Two attacks on rank metric code-based schemes: RankSign and an Identity-Based-Encryption scheme

Thomas Debris-Alazard *† Jean-Pierre Tillich †

May 17, 2018

Abstract

RankSign [GRSZ14] is a code-based signature scheme proposed to the NIST competition for quantum-safe cryptography [AGH+17] and, moreover, is a fundamental building block of a new Identity-Based-Encryption (IBE) [GHPT17]. This signature scheme is based on the rank metric and enjoys remarkably small key sizes, about 10KBytes for an intended level of security of 128 bits. Unfortunately we will show that all the parameters proposed for this scheme in [AGH+17] can be broken by an algebraic attack that exploits the fact that the augmented LRPC codes used in this scheme have very low weight codewords. Therefore, without RankSign the IBE cannot be instantiated at this time. As a second contribution we will show that the problem is deeper than finding a new signature in rank-based cryptography, we also found an attack on the generic problem upon which its security reduction relies. However, contrarily to the RankSign scheme, it seems that the parameters of the IBE scheme could be chosen in order to avoid our attack. Finally, we have also shown that if one replaces the rank metric in the [GHPT17] IBE scheme by the Hamming metric, then a devastating attack can be found.

1 Introduction

1.1 An efficient code-based signature scheme: RankSign and a code-based Identity-Based-Encryption scheme

Code-based signature schemes. It is a long standing open problem to build an efficient and secure signature scheme based on the hardness of decoding a linear code which could compete in all respects with DSA or RSA. Such schemes could indeed give a quantum resistant signature for replacing in practice the aforementioned signature schemes that are well known to be broken by quantum computers. A first partial answer to this question was given in [CFS01]. It consisted in adapting the Niederreiter scheme [Nie86] for this purpose. This requires a linear code for which there exists an efficient decoding algorithm for a non-negligible set of inputs. This means that if $\mathbf{H}$ is an $r \times n$ parity-check matrix of the code, there exists for a non-negligible set of elements $\mathbf{s}$ in $\{0,1\}^r$ an efficient way to find a word $\mathbf{e}$ in $\{0,1\}^n$ of smallest Hamming weight such that $\mathbf{He}^\intercal = \mathbf{s}^\intercal$.

The authors of [CFS01] noticed that very high rate Goppa codes are able to fulfill this task, and their scheme can indeed be considered as the first step towards a solution of the aforementioned problem. However, the poor scaling of the key size when security has to be increased prevents this scheme to be a completely satisfying answer to this issue.

The rank metric. There has been some exciting progress in this area for another metric, namely the rank metric [GRSZ14]. A code-based signature scheme whose security relies on decoding codes with respect to the rank metric has been proposed there. It is called RankSign. Strictly speaking,

*Sorbonne Universités, UPMC Univ Paris 06, France
†Inria, SECRET Project, 2 Rue Simone Iff 75012 Paris Cedex

the rank metric consists in viewing an element in $\mathbb{F}_q^N$ (when N is a product $N = m \times n$) as an $m \times n$ matrix over $\mathbb{F}_q$ and the rank distance between two elements $\mathbf{x}$ and $\mathbf{y}$ is defined as the rank of the matrix $\mathbf{x} - \mathbf{y}$. This depends of course on how N is viewed as a product of two elements. Decoding in this metric is known to be an NP hard problem [BFS99, Cou01]. In the particular case of [GRSZ14], the codes which are considered are not $\mathbb{F}_q$-linear but, as is customary in the setting of rank metric based cryptography, $\mathbb{F}_{q^m}$-linear: the codes are here subspaces of $\mathbb{F}_{q^m}^n$. Here the elements $\mathbf{x} = (x_1, \ldots, x_n)$ of $\mathbb{F}_{q^m}^n$ are viewed as $m \times n$ matrices by expressing each coordinate x_i in a certain fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. This yields a column vector $\mathbf{x}^i$ in $\mathbb{F}_q^m$ and the concatenation of these column vectors yields an $m \times n$ matrix $\mathbf{Mat}(\mathbf{x}) = \begin{pmatrix} \mathbf{x}^1 & \ldots & \mathbf{x}^n \end{pmatrix}$ that allows to put a rank metric over $\mathbb{F}_{q^m}^n$. This allows to reduce the key size by a factor of m when compared to the $\mathbb{F}_q$-linear setting (for more details see the paragraph at the end of Section 2).

Decoding such codes for the rank metric is not known to be NP-hard anymore. There is however a randomized reduction of this problem to decode an $\mathbb{F}_q$-linear code for the Hamming metric [GZ16] when the degree m of the extension field is sufficiently big. This situation is in some sense reminiscent to the current thread in cryptography based on codes or on lattices where structured codes (for instance quasi-cyclic codes) or structured lattices (corresponding to an additional ring structure) are taken. However the $\mathbb{F}_{q^m}$-linear case has an advantage over the other structured proposals, in the sense that it has a randomized reduction to an NP complete problem. This is not the case for the other structured proposals. Relying on $\mathbb{F}_{q^m}$-linear codes is one of the main reason why RankSign enjoys noticeably small public key sizes: it is about 10KBytes for 128 bits of security for the parameters proposed in the NIST submission[AGH$^+$17]. Furthermore, RankSign comes with a security proof showing that there is no leakage coming from signing many times. It also proved to be a fundamental building block in the Identity-Based-Encryption (IBE) scheme based on the rank metric suggested in [GHPT17].

A new IBE scheme based on codes. The concept of IBE was introduced by Shamir in 1984 [Sha84]. It gives an alternative to the standard notion of public-key encryption. In an IBE scheme, the public key associated with a user can be an arbitrary identity string, such as his e-mail address, and others can send encrypted messages to a user using his identity without having to rely on a public-key infrastructure, given short public parameters. The main technical difference between a Public Key Encryption (PKE) and IBE is the way the public and private keys are bound and the way of verifying those keys. In a PKE scheme, verification is achieved through the use of a certificate which relies on a public-key infrastructure. In an IBE, there is no need of verification of the public key but the private key is managed by a Trusted Authority (TA).

There are two issues that makes the design of IBE extremely hard: the requirement that public keys are arbitrary strings and the ability to extract decryption keys from the public keys. In fact, it took nearly twenty years for the problem of designing an efficient method to implement an IBE to be solved. The known methods of designing IBE are based on different tools: from elliptic curve pairings [SOK00] and [BF01]; from the quadratic residue problem [Cou01]; from the Learning-With-Error (LWE) problem [GPV08]; from the computational Diffie-Hellman assumption [DG17b] and finally from the Rank Support Learning (RSL) problem [GHPT17]. The last scheme based on codes is an adaptation of the [GPV08] technique, but instead of relying on the Hamming metric it relies on the rank metric. It has to be noted that there has been some recent and exciting progress in the design of IBE. In [DG17a] it has been shown how to generalize the work of [DG17b] by introducing a new primitive, One-Time Signatures with Encryption (OTSE), that enables to construct fully secure IBE schemes. Furthermore it was shown in [DGHM18] how to instantiate OTSE primitives from LWE and the Low Parity Noise problems (LPN). This gave after the IBE's [GPV08] and [GHPT17] the third scheme which may hope to resist to a quantum computer.

1.2 Our contribution

An efficient attack on RankSign. Our first contribution is that despite the fact that the security of RankSign might very well be founded on a hard problem (namely distinguishing an

augmented LRPC code from a random linear code), we show here that all the parameters proposed for RankSign in [AGH+17] can be broken by a suitable algebraic attack. The problem is actually deeper than that, because the attack is actually polynomial in nature and can not really be thwarted by changing the parameters. The attack builds upon the following observations

- The RankSign scheme is based on augmented LRPC codes;
- To have an efficient signature scheme, the parameters of the augmented LRPC codes have to be chosen very carefully;
- For the whole range of admissible parameters, it turns out rather unexpectedly that these augmented LRPC codes have very low-weight codewords. This can be proved by subspace product considerations;
- These low-weight codewords can be recovered by algebraic techniques and reveal enough of the secret trapdoor used in the scheme to be able to sign like a legitimate user.

This attack has also a significant impact on the IBE proposal [GHPT17] whose security is based on the security of RankSign. Right now, there is no backup solution for instantiating this IBE scheme, since RankSign was the only rank-metric code based signature scheme following the hash and sign paradigm that is needed in the IBE scheme.

An efficient attack on the IBE [GHPT17]. Our second contribution is to show that the problem is deeper than finding a new hash and sign signature scheme in rank-based cryptography to instantiate the IBE proposed in [GHPT17]. Actually the security of this IBE scheme does not solely rely on the rank metric code-based signature scheme and the rank syndrome decoding, it also relies on the Rank Support Learning (RSL) problem. We show here that the RSL problem is much easier for the parameters proposed in the IBE scheme [GHPT17] and can be broken by a suitable algebraic attack. Interestingly enough, the approach for breaking the RSL problem is similar to what we did for RankSign:

- we exhibit a matrix code that can be deduced from the public data that contains many low-weight codewords and whose support reveals the secret support of the RSL problem;
- we find such low weight codewords efficiently by solving a largely overdetermined bilinear system.

However in this case, contrarily to the RankSign scheme, even if the set of parameters that could defeat our attack is small, it is non empty and our attack could be thwarted by choosing the parameters appropriately and if an appropriate signature scheme were found.

We have also explored whether it is possible to change in the IBE scheme of [GHPT17] the rank metric by the Hamming metric. It turns out that the problem is much worse for the Hamming case. Indeed by adapting the IBE [GHPT17] to the Hamming metric, based on the remark that signatures must have a small weight, we show that even the simplest generic attack, namely the Prange algorithm [Pra62], breaks the IBE in the Hamming setting in polynomial time, and this irrespective of the way the parameters are chosen.

2 Generalities on rank metric and $\mathbb{F}_{q^m}$-linear codes

2.1 Definitions and notation

We provide here notation and definitions that are used throughout the paper.

Vector notation. Vectors will be written using bold lower-case letters, e.g. $\mathbf{x}$. The ith component of $\mathbf{x}$ is denoted by x_i. Vectors are in row notation. Matrices will be written as bold capital letters, e.g. $\mathbf{X}$, and the i-th column of a matrix $\mathbf{X}$ is denoted $\mathbf{X}_i$. The rank of a matrix $\mathbf{X}$ will be

simply denoted by $|\mathbf{X}|$.

Field notation. Let q be a power of a prime number. We will denote by $\mathbb{F}_q$ the finite field of cardinality q.

Coding theory notation. A linear code $\mathscr{C}$ over a finite field $\mathbb{F}_q$ of length n and dimension k is a subspace of the vector space $\mathbb{F}_q^n$ of dimension k. We say that it has parameters $[n,k]$ or that it is an $[n,k]$-code. A generator matrix $\mathbf{G}$ for it is a full rank $k \times n$ matrix over $\mathbb{F}_q$ which is such that

$$\mathscr{C} = \{\mathbf{uG} : \mathbf{u} \in \mathbb{F}_q^k\}.$$

In other words, the rows of $\mathbf{G}$ form a basis of $\mathscr{C}$. A parity-check matrix $\mathbf{H}$ for it is a full-rank $(n-k) \times n$ matrix over $\mathbb{F}_q$ such that

$$\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{Hc}^\intercal = 0\}.$$

In other words, $\mathscr{C}$ is the null space of $\mathbf{H}$.

Rank metric codes basically consist in viewing codewords as matrices. More precisely, when N is the product of two numbers m and n, $N = mn$ we will equip the vector space $\mathbb{F}_q^N$ with the rank metric by viewing its elements as matrices over $\mathbb{F}_q^{m\times n}$, i.e.

$$d(\mathbf{X}, \mathbf{Y}) = |\mathbf{X} - \mathbf{Y}|.$$

An $[m \times n, K]$ *matrix code* of dimension K over $\mathbb{F}_q^{m\times n}$ is a subspace of $\mathbb{F}_q^{m\times n}$ of dimension K. Such a code is equipped in a natural way with the rank metric. There is a particular subclass of matrix codes that has the nice property to be specified much more compactly than a generic matrix code. It consists in taking a linear code over an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ of length n. Such a code can be viewed as a matrix code consisting of matrices in $\mathbb{F}_q^{m\times n}$ by expressing each coordinate c_i of a codeword $\mathbf{c} = (c_i)_{1\le i\le n}$ in a fixed $\mathbb{F}_q$ basis of $\mathbb{F}_{q^m}$. When the $\mathbb{F}_{q^m}$-linear code is of dimension k the dimension of the matrix code viewed as an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$ is $K = k.m$. More precisely we bring in the following definition.

Definition 1 (Matrix code associated to an $\mathbb{F}_{q^m}$ linear code)**.** *Let $\mathscr{C}$ be an $[n,k]$-linear code over $\mathbb{F}_{q^m}$, that is a subspace of $\mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$, and let $(\beta_1 \dots \beta_m)$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Each word $\mathbf{c} \in \mathscr{C}$ can be represented by an $m \times n$ matrix $\mathbf{Mat}(\mathbf{c}) = (M_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$ over $\mathbb{F}_q$, with $c_j = \sum_{i=1}^m M_{ij}\beta_i$. The set $\{\mathbf{Mat}(\mathbf{c}), \mathbf{c} \in \mathscr{C}\}$ is the $[m \times n, k.m]$ matrix code over $\mathbb{F}_q$ associated to the $\mathbb{F}_{q^m}$ linear code $\mathscr{C}$. The (rank) weight of $\mathbf{c}$ is defined as the rank of the associated matrix, that is $|\mathbf{c}| \stackrel{\triangle}{=} |\mathbf{Mat}(\mathbf{c})|$.*

This definition depends of course on the basis chosen for $\mathbb{F}_{q^m}$. However changing the basis does not change the distance between codewords. The point of defining matrix codes in this way is that they have a more compact description. It is readily seen that an $[m \times n, k.m]$ matrix code over $\mathbb{F}_q$ can be specified from a systematic generator matrix (i.e. a matrix of the form $\left[\mathbf{1}_{k.m}|\mathbf{P}\right]$ with $\mathbf{1}_{k.m}$ being the identity matrix of size $k.m$) by $k(n-k)m^2 \log_2 q$ bits whereas an $\mathbb{F}_{q^m}$-linear code uses only $k(n-k)\log_2 q^m = k(n-k)m \log_2 q$ bits. This is particularly interesting for cryptographic applications where this notion is directly related to the public key size. This is basically what explains why in general McEliece cryptosystems based on rank metric matrix codes have a smaller keysize than McEliece cryptosystems based on the Hamming metric. All of these proposals (see for instance [GPT91, GO01, Gab08, GMRZ13, GRSZ14, ABD$^+$17b, AMAB$^+$17]) are actually built from matrix codes over $\mathbb{F}_q$ obtained from $\mathbb{F}_{q^m}$-linear codes. In a sense, they can be viewed as structured matrix codes, much in the same way as quasi-cyclic linear codes can be viewed as structured versions of linear codes. In the latter case, the code is globally invariant by a linear isometric transform on the codewords corresponding to shifts of a certain length. In the $\mathbb{F}_{q^m}$ linear case the code is globally invariant by an isometric linear transformation that corresponds to multiplication in $\mathbb{F}_{q^m}$.

2.2 Rank code-based cryptography

Rank-based cryptography relies on the hardness of decoding for the rank metric. This problem is the rank metric analogue of the well known decoding problem in the Hamming metric [BMvT78]. We give it here its syndrome formulation:

Problem 1 (Rank (Metric) Syndrome Decoding Problem)**.**
Instance: A full-rank $(n-k) \times n$ *matrix* $\mathbf{H}$ *over* $\mathbb{F}_{q^m}$ *with* $k \leq n$*, a syndrome* $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ *and* w *an integer.*
Output: An error $\mathbf{e} \in \mathbb{F}_{q^m}^n$ *such that* $|\mathbf{e}| = w$ *and* $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$*.*

This problem has recently been proven hard in [GZ16] by a probabilistic reduction to the decoding problem in the Hamming metric which is known to be NP-complete [BMvT78]. This problem has typically a unique solution when w is below the Varshamov-Gilbert distance $w_{\mathrm{rVG}}(q, m, n, k)$ for the rank metric which is defined as

Definition 2 (Varshamov-Gilbert distance for the rank metric)**.** *The Varshamov-Gilbert distance* $w_{\mathrm{rVG}}(q, m, n, k)$ *for* $\mathbb{F}_{q^m}$ *linear codes of dimension* k *in the rank metric is defined as the smallest* t *for which* $q^{m(n-k)} \geq B_t$ *where* B_t *is the size of the ball of radius* t *in the rank metric.*

Remark 1.

1. $q^{m(n-k)}$ *can be viewed as the number of different syndromes* $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$*.*
2. $B_t = \sum_{i=0}^{t} S_i$ *where* S_i *is the size of a sphere of radius* i *in the rank metric over* $\mathbb{F}_q^{m \times n}$*. This latter quantity is equal to*
$$S_i = \prod_{j=0}^{i-1} \frac{(q^n - q^j)(q^m - q^j)}{(q^i - q^j)} = \Theta\left(q^{i(m+n-i)}\right).$$
3. *From this last asymptotic expression it is straightforward to check that (for more details see [Loi14])*
$$w_{\mathrm{rVG}}(q, m, n, k) = \frac{m + n - \sqrt{(m-n)^2 + 4km}}{2}(1 + o(1)),$$
when either m *or* n *tends to infinity.*

The best algorithms for solving the decoding problem in the rank metric are exponential in n^2 as long as $m = \Theta(n)$, $w = \Theta(n)$ but stays below the Singleton bound which is defined by

Definition 3 (Singleton distance in the rank metric)**.** *The rank Singleton distance* $w_{\mathrm{rS}}(q, m, n, k)$ *for* $\mathbb{F}_{q^m}$ *linear codes of dimension* k *is defined as* $w_{\mathrm{rS}}(q, m, n, k) \stackrel{\triangle}{=} \left\lfloor \frac{(n-k)m}{\max(m,n)} \right\rfloor + 1$

The usual notion of the support of a vector is generally relevant to decoding in the Hamming metric and corresponds for a vector $\mathbf{x} = (x_i)_{1 \leq i \leq n}$ to the set of positions i in $\{1, \ldots, n\}$ such that $x_i \neq 0$. Various decoding algorithms for the Hamming metric [Pra62, LB88, Ste88, Dum91, FS09, BLP11, MMT11, BJMM12, MO15, DT17, BM17] use this notion in a rather fundamental way. The definition of the support of a vector has to be changed a little bit to be relevant to the rank metric. This notion was first put forward in [GRS13, GRS16] to obtain an analogue of the Prange decoder [Pra62] for the rank metric.

Definition 4 (Support)**.** *Let* $\mathbf{x} = (x_i)_{1 \leq i \leq n}$ *be a vector of* $\mathbb{F}_{q^m}^n$*, its support is defined as:*

$$\mathrm{Supp}(\mathbf{x}) \stackrel{\triangle}{=} \langle x_1, \cdots, x_n \rangle_{\mathbb{F}_q}.$$

This notion of support is among other things relied to the rank metric as it is easily verified that for any vector $\mathbf{x}$ of $\mathbb{F}_{q^m}^n$ we have:

$$|\mathbf{x}| = \dim(\mathrm{Supp}(\mathbf{x}))$$

3 The RankSign scheme

We recall in this section basic facts about RankSign [GRSZ14]. It is based on augmented LRPC codes. Roughly speaking it is a hash and sign signature scheme: the message $\mathbf{m}$ that has to be signed is hashed by a hash function $\mathscr{H}$ and the signature is equal to $f^{-1}(\mathscr{H}(\mathbf{m}))$ where f is a trapdoor one-way function. In this way the pair $(\mathbf{m}, f^{-1}(\mathscr{H}(\mathbf{m})))$ forms a valid signature. Recall now that code-based cryptography relies on Problem 1 (rank syndrome decoding) which amounts to consider here the following one way-function to build a signature primitive:

$$\begin{array}{rccc} f_{\mathbf{H}}: & S_w & \longrightarrow & \mathbb{F}_{q^m}^{n-k} \\ & \mathbf{e} & \longmapsto & \mathbf{e}\mathbf{H}^\intercal \end{array}$$

where S_w denotes the words of $\mathbb{F}_{q^m}^n$ of rank weight w, $\mathbf{H}$ a parity-check matrix of size $(n-k)\times n$. To introduce a trapdoor in $f_{\mathbf{H}}$ authors of [GMRZ13] proposed to use parity-check matrices of the family of augmented LRPC codes. Indeed, when the underlying LRPC structure is known (roughly speaking, this is the trapdoor), there is a decoding algorithm based on the LRPC structure that computes for any (or for a good fraction) $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ an $\mathbf{e} \in \mathbb{F}_{q^m}^n$ of weight w such that $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$. This decoding algorithm is probabilistic and the parameters of the code have to be chosen in a very specific fashion in order to have a probability of success very close to 1 (see Fact 1 at the end of this section).
The following definition will be useful for our discussion.

Definition 5 (Homogeneous Matrix)**.** *A matrix $\mathbf{H} = (H_{ij})_{\substack{1\le i\le n-k \\ 1\le j\le n}}$ over $\mathbb{F}_{q^m}$ is homogeneous of weight d if all its coefficients generate an $\mathbb{F}_q$-vector space of dimension d:*

$$\dim\left(\langle H_{ij} : 1 \le i \le n-k,\ 1 \le j \le n\rangle_{\mathbb{F}_q}\right) = d$$

LRPC (Low Rank Parity Check) codes of weight d and augmented LRPC codes of type (d,t) are defined from homogeneous matrices of weight d as

Definition 6 (LRPC and augmented LRPC code)**.** *An* LRPC *code over $\mathbb{F}_{q^m}$ of weight d is a code that admits a parity-check matrix $\mathbf{H}$ with entries in $\mathbb{F}_{q^m}$ that is homogeneous of weight d whereas an augmented* LRPC *code of type (d,t) over $\mathbb{F}_{q^m}$ is a code that admits a parity-check matrix $\mathbf{H}' = \big[\mathbf{H}|\mathbf{R}\big]\,\mathbf{P}$ where $\mathbf{H}$ is a homogeneous matrix of rank d over $\mathbb{F}_{q^m}$, $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$ and $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$.*

Remark 2. *Note that $\mathbf{P} \in \mathbb{F}_q^{n\times n}$ is an isometry for the rank metric, since for any $\mathbf{x} \in \mathbb{F}_{q^m}^n$ we have* $\mathrm{Supp}(\mathbf{x}) = \mathrm{Supp}(\mathbf{x}\mathbf{P})$ *and therefore*

$$|\mathbf{x}| = |\mathbf{x}\mathbf{P}|.$$

The public key and the secret key for RankSign are given by:

public key: $\mathbf{H}_{\mathrm{pub}}$ which is a random $(n-k)\times n$ parity-check matrix of an augmented LRPC code of type (d,t). It is of the form

$$\mathbf{H}_{\mathrm{pub}} = \mathbf{Q}\mathbf{H}'$$

with $\mathbf{H}' = \big[\mathbf{H}|\mathbf{R}\big]\,\mathbf{P}$ where $\mathbf{Q}$ is an invertible $(n-k)\times(n-k)$ matrix over $\mathbb{F}_{q^m}$, $\mathbf{H}$ is a homogeneous matrix of rank d over $\mathbb{F}_{q^m}$, $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$ and $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$.

secret key: The matrix $\mathbf{H}_{\mathrm{sec}} \triangleq \big[\mathbf{H}|\mathbf{R}\big]$.

From the knowledge of this last matrix a signature is computed by using a decoding algorithm devised for LRPC codes. Recall that LRPC codes can be viewed as analogues of LDPC codes for

the rank metric. In particular, they enjoy an efficient decoding algorithm based on their low rank parity-check matrix. Roughly speaking, Algorithm 1 of [GMRZ13] decodes up to w errors when $dw \leq n-k$ in polynomial time (see [GMRZ13, Theorem 1]). It uses in a crucial way the notion of the linear span of a product of subspaces of $\mathbb{F}_{q^m}$:

Definition 7. *Let U and V be two subspaces of $\mathbb{F}_{q^m}$, then*

$$U \cdot V \stackrel{\triangle}{=} \langle uv : u \in U,\ v \in V \rangle_{\mathbb{F}_q}.$$

Roughly speaking, Algorithm 1 of [GMRZ13] works as follows when we have to recover an error $\mathbf{e}$ of weight w from the knowledge of its syndrome $\mathbf{s}$ with respect to a parity-check matrix $\mathbf{H} = (H_{ij})_{\substack{1 \leq i \leq n-k \\ 1 \leq j \leq n}}$ over $\mathbb{F}_{q^m}$ that is homogeneous of weight d, that is

$$\mathbf{s}^\intercal = \mathbf{H}\mathbf{e}^\intercal. \tag{1}$$

1. Let $U \stackrel{\triangle}{=} \langle H_{ij} : 1 \leq i \leq n-k,\ 1 \leq j \leq n \rangle_{\mathbb{F}_q}$, $V \stackrel{\triangle}{=} \mathrm{Supp}(\mathbf{e})$ and $W \stackrel{\triangle}{=} \mathrm{Supp}(\mathbf{s})$. U and W are known, whereas V is unknown to the decoder. By definition U is of dimension d and it is convenient to bring in a basis $\{f_1, \ldots, f_d\}$ for it.

2. It turns out that we typically have $W = U \cdot V$. Moreover it is clear that in such a case $V \subset f_1^{-1}W \cap f_2^{-1}W \cdots f_d^{-1}W$. It also turns out that we typically have

   $$V = f_1^{-1}W \cap f_2^{-1}W \cdots f_d^{-1}W.$$

   V is therefore computed by taking the intersection of all the $f_i^{-1}W$'s.

3. Once we have the support of $\mathbf{e}$ ($V = \mathrm{Supp}(\mathbf{e})$), the error $\mathbf{e} = (e_1, \ldots, e_n)$ can be recovered by solving the linear equation $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$ with the additional constraints $e_i \in \mathrm{Supp}(\mathbf{e})$ for $i \in \{1, \ldots, n\}$. There are in this case enough linear constraints to recover a unique $\mathbf{e}$.

The last algorithm seems to apply when there is a unique solution to (1). It can also be used with a slight modification (by adding "erasures" [GRSZ14]) for weights for which there are many solutions to it (this is typically the regime which is used for the RankSign scheme). It namely turns out, see [GRSZ14], that this decoder can for a certain range of parameters be used for a large fraction of possible syndromes $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ to produce an error $\mathbf{e}$ of weight w that satisfies (1). It can even be required that $\mathrm{Supp}(\mathbf{e})$ contains a subspace T of some dimension t. Furthermore this procedure can also be generalized to a parity-check matrix of an augmented LRPC code. More precisely to summarize the discussion that can be found in [GRSZ14, AGH$^+$17]

Fact 1. *Let $\mathbf{H}$ be a random homogeneous matrix of weight d in $\mathbb{F}_{q^m}^{(n-k)\times n}$, $\mathbf{H}' = \left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}$ where $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$ and $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$. There is a probabilistic polynomial time algorithm that outputs for a large fraction of syndromes $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$, subspaces T of $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$–dimension t', an error $\mathbf{e}$ of weight w whose support contains the subspace T that satisfies*

$$\mathbf{H}'\mathbf{e}^\intercal = \mathbf{s}^\intercal$$

as soon as the parameters n, k, t, t', d, w satisfy

$$\begin{aligned} m &= (w - t')(d+1) && (2)\\ n-k &= d(w - t - t') && (3)\\ n &= (n-k)d. && (4) \end{aligned}$$

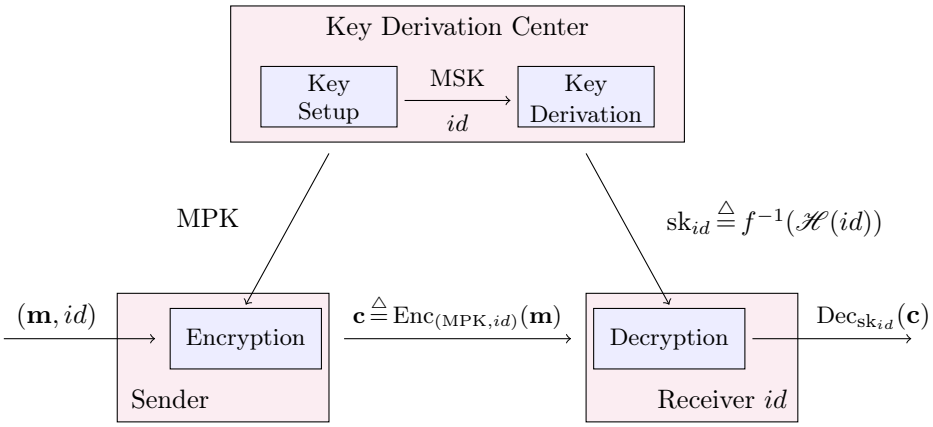

Figure 1: IBE in the GPV context

4 Identity-Based-Encryption in code-based cryptography

We recall in this section the [GHPT17] approach for obtaining an IBE scheme whose security relies on code-based assumptions. In some sense, this scheme can be viewed as an adaptation of the first quantum-safe IBE which was introduced by [GPV08] in the paradigm of lattice-based cryptography. It relies among other things on two fundamental building blocks: a hash and sign primitive and an encryption scheme related to it. The adaptation relies on two building blocks: *i*) a signature scheme, RankSign whose security relies on code-based assumptions for the rank metric, *ii*) a new encryption scheme, namely RankPKE [GHPT17], based on the Rank Support Leaning (RSL) problem. [GHPT17] gives a security proof of the IBE scheme that relies on two assumptions: *i*) the key security of RankSign and *ii*) the difficulty of RSL. Furthermore, the work of [GHPT17] can be easily generalized to the more common Hamming metric. It is why we present in what follows the [GHPT17] IBE scheme with codes independently of the metric.

Roughly speaking, an IBE is a specific public-key encryption scheme that allows senders to encrypt messages thanks to the receiver's identity (such as its email address). To permit this protocol there is a third party, say a Key Derivation Center, which owns a master secret-key MSK and an associated public-key MPK that allows to compute from *any* identity id a related secret quantity sk_{id} that will be used in a public-key encryption scheme involving an arbitrary sender and the receiver of identity id, with the pair of public/secret key $((id, \mathrm{MPK}), \mathrm{sk}_{id})$. In this paradigm any identity id needs to be matched with a secret key sk_{id} and to achieve this goal it was proposed in [GPV08] to use a hash and sign primitive. Roughly speaking, for a trapdoor function f and a hash function $\mathscr{H}$ the Key Derivation Center will compute from id the quantity $f^{-1}(\mathscr{H}(id))$ which will be used as sk_{id}. We summarize in Figure 1 how this IBE works. In the case of [GPV08], signatures sample short vectors whose addition with the hash of the identity gives lattice points. Then this is used as a secret-key of an encryption scheme whose security relies on the hardness of the LWE problem (see [GPV08, Section 7.1, p26]).

IBE in code-based cryptography. We give now the general framework of [GHPT17] for obtaining a code-based IBE scheme. It is only given in the rank metric case in [GHPT17], but the approach is really more general than this and can be given for the Hamming metric too. We will detail what happens for both metrics here. As explained above, this scheme builds upon a hash and sign primitive and the authors of [GHPT17] proposed RankSign there but in our description the signature scheme is just a black-box.

Let $\mathscr{C}_{\mathrm{sgn}}$ be a code of length n_{sgn} and dimension k_{sgn} for which there is a trapdoor that enables to compute for any $\mathbf{y} \in \mathbb{F}_2^{n_{\mathrm{sgn}}}$ a codeword $\mathbf{c}_{\mathbf{y}} \in \mathscr{C}_{\mathrm{sgn}}$ at distance w_{sgn}. Let d be an integer, $\mathscr{C}_{\mathrm{dec}}$ be a code of length N_{dec} and dimension k_{dec} such that it exists a polynomial algorithm to decode a linear (in the length) error weight. Let $\mathbf{G}_{\mathscr{C}_{\mathrm{sgn}}}$ and $\mathbf{G}_{\mathscr{C}_{\mathrm{dec}}}$ be generator matrices of the codes $\mathscr{C}_{\mathrm{sgn}}$

and $\mathscr{C}_{\text{dec}}$ respectively. Then it is proposed in [GHPT17] to set master secret and public keys as:

- MSK be the trapdoor which enables to decode at distance w_{sgn} in $\mathscr{C}_{\text{sgn}}$;
- $\text{MPK} \stackrel{\triangle}{=} (\mathscr{C}_{\text{sgn}}, \mathscr{C}_{\text{dec}})$.

Let id be an identity and $\mathscr{H}$ be a hash function whose range is $\mathbb{F}_2^{n_{\text{sgn}}}$ or $\mathbb{F}_{q^m}^{n_{\text{sgn}}}$ according to the metric which is used. The key derivation center computes with MSK and id a vector $\mathbf{u}_{id}$ such that:

$$|\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)| = w_{\text{sgn}} \text{ where } |\cdot| \text{ denotes either the Hamming or rank metric} \tag{5}$$

This is used as the secret key associated to the identity id:

- $\text{sk}_{id} \stackrel{\triangle}{=} \mathbf{u}_{id}$.

We are now ready to present the encryption scheme whose public/secret key is $((\mathbf{G}_{\mathscr{C}_{\text{sgn}}}, \mathbf{G}_{\mathscr{C}_{\text{dec}}}, id), \mathbf{u}_{id})$ and which in the particular case of the rank metric is the RankPKE scheme introduced in [GHPT17]. This primitive is related to the work of Alekhnovich [Ale11].

- **Encryption.** Let $\mathbf{m}$ be the message that will be encrypted. We will denote by $\mathbb{F}$ the finite field $\mathbb{F}_2$ or $\mathbb{F}_{q^m}$ depending on the Hamming or rank metric. The authors of [GHPT17] introduced the trapdoor function:

$$\begin{array}{rccc} g_{\mathbf{G}_{\mathscr{C}_{\text{sgn}}}, \mathbf{G}_{\mathscr{C}_{\text{dec}}}, id}: & \mathbb{F}^{k_{\text{dec}}} & \longrightarrow & \mathbb{F}^{(k_{\text{sgn}}+1)\times N_{\text{dec}}} \\ & \mathbf{m} & \longmapsto & \begin{bmatrix} \mathbf{G}_{\mathscr{C}_{\text{sgn}}}\mathbf{E} \\ \mathscr{H}(id)\mathbf{E} + \mathbf{m}\mathbf{G}_{\mathscr{C}_{\text{dec}}} \end{bmatrix} \end{array}$$

  where $\mathbf{E}$ has a size $n_{\text{sgn}} \times N_{\text{dec}}$. In the case of the rank metric $\mathbf{E}$ is a matrix uniformly picked at random among the homogeneous matrices of weight d and in the case of the Hamming metric, $\mathbf{E}$ is picked uniformly at random among the matrices whose columns have all weight d.

- **Decryption.** The secret key $\mathbf{u}_{id}$ is used as

$$\begin{aligned} (\mathbf{u}_{id}, -1) g_{\mathbf{G}_{\mathscr{C}_{\text{sgn}}}, \mathbf{G}_{\mathscr{C}_{\text{dec}}}, id}(\mathbf{m}) &= (\mathbf{u}_{id}, -1) \begin{bmatrix} \mathbf{G}_{\mathscr{C}_{\text{sgn}}}\mathbf{E} \\ \mathscr{H}(id)\mathbf{E} + \mathbf{m}\mathbf{G}_{\mathscr{C}_{\text{dec}}} \end{bmatrix} \\ &= \left(\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)\right)\mathbf{E} - \mathbf{m}\mathbf{G}_{\mathscr{C}_{\text{dec}}} \end{aligned}$$

  It can be verified that under certain restrictions on w_{sgn} and d, the weight of the vector $\left(\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)\right)\mathbf{E}$ is low enough, so that a decoding algorithm for $\mathscr{C}_{\text{dec}}$ will recover $\mathbf{m}$. The following proposition gives a constraint on these parameters so that decoding is possible in principle.

  Proposition 1. *In order to be able to decode asymptotically at constant rate R, there should exist an $\varepsilon(R) > 0$ such that all the parameters $n_{\text{sgn}}, w_{\text{sgn}}$ and d have to verify*

  - *in the rank metric case*

$$w_{\text{sgn}} d = (1 - \varepsilon(R)) \min(m, N_{\text{dec}}) \tag{6}$$

  - *in the Hamming metric case*

$$w_{\text{sgn}} d = O(n_{\text{sgn}}). \tag{7}$$

Proof. We separate the proof in two parts.

Rank metric. In this case, as proved in [GHPT17, §3.2] the rank weight of the error term $\left(\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)\right)\mathbf{E}$ is with high probability $w_{\text{sgn}}d$. Recall that $\mathscr{C}_{\text{dec}}$ is a code over the alphabet $\mathbb{F}_{q^m}$. A necessary condition to be able to decode with a fixed rate code is that the dimension of the support of the error is at most some fraction of the dimension m of the whole space $\mathbb{F}_{q^m}$ and of the length N_{dec} of the code we decode. This means that $wd \leq (1-\varepsilon(R))\min(m, N_{\text{dec}})$.

Hamming metric. Recall that $\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)$ has Hamming weight w_{sgn} (see (5)). It is easily verified that the probability for one bit of $\left(\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)\right)\mathbf{E}$ to be equal to 1 is of the form $(1/2)(1-e^{-2wd/n(1+O(1))})$ when the columns of $\mathbf{E}$ are picked uniformly at random among the words of Hamming weight d. Furthermore the relative weight of $\left(\mathbf{u}_{id}\mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)\right)\mathbf{E}$ concentrates around this probability and a necessary condition to be able to decode at constant rate asymptotically is that this relative weight is a constant $< 1/2$. Therefore it is necessary to have $w_{\text{sgn}}d = O(n_{\text{sgn}})$.

□

The constraint set on the parameters by this proposition is crucial to instantiate the IBE in code-based cryptography. Unfortunately, this constraint implies a fatal weakness for the Hamming based scheme and a hard to meet condition for the rank metric in order to have a secure scheme as we will see in what follows.

The RSL problem. We recall here the assumption upon which the security of RankPKE relies (the previous encryption scheme in rank metric), namely the Rank Support Leaning (RSL) problem introduced in [GHPT17]. This problem is a rank syndrome decoding problem with syndromes that are associated to errors that all share the same support which is the secret.

Problem 2 (RSL - Rank Support Learning)**.**
Parameters: n, k, N, d
Instance: $(\mathbf{A}, \mathbf{AE})$ *where* $\mathbf{A}$ *is a full rank matrix of size* $(n-k)\times n$, $\mathbf{E}$ *a matrix of size* $n \times N$ *where all its coefficients belong to a same subspace* F *of* $\mathbb{F}_{q^m}$ *of dimension* d
Output: the subspace F.
The decisional version of RSL*, namely* DRSL*, is to distinguish distributions* $(\mathbf{A}, \mathbf{AE})$ *from* $(\mathbf{A}, \mathbf{R})$ *where* $\mathbf{A}, \mathbf{R}$ *and* $\mathbf{E}$ *are random variables whose distribution is uniform over matrices of size* $(n-k)\times n, (n-k)\times N$ *and over homogeneous matrices of size* $n \times N$.

Remark 3. *Let* $(\mathbf{A}, \mathbf{AE})$ *be an instance of* RSL*. The matrix* $\mathbf{A}$ *is of full-rank of size* $(n-k)\times n$ *and we can perform Gaussian elimination on its rows to get a matrix* $\mathbf{S}$ *such that* $\mathbf{SA} = [I_{n-k}|\mathbf{A}']$. *The pair* $(\mathbf{SA}, \mathbf{SAE})$ *is still an instance of RSL with the same parameters and secret subspace* F*, it is why we can always assume that for any instance of RSL the matrix* $\mathbf{A}$ *is in systematic form.*

As proved in [GHPT17, §3.3, p13, Theorem 1] the security of RankPKE relies on the DRSL problem.

5 Attack on RankSign

5.1 The problem with RankSign : low rank codewords in the augmented LRPC code

A natural way to attack RankSign is to find low weight codewords in the dual of the augmented LRPC code. Recall that the public parity-check matrix used in the scheme is a matrix $\mathbf{H}_{\text{pub}}$ where

$$\mathbf{H}_{\text{pub}} = \mathbf{QH}'$$

with $\mathbf{H}' = \left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}$ where $\mathbf{H}$ is a homogeneous matrix of rank d over $\mathbb{F}_{q^m}$, $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$, $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has

the same number of columns as $\mathbf{H}'$ and $\mathbf{Q}$ is a square and invertible matrix over $\mathbb{F}_{q^m}$ which has the same number of rows as $\mathbf{H}'$. If we call $\mathscr{C}_{\text{pub}}$ the "public code" with parity-check matrix $\mathbf{H}_{\text{pub}}$, then the dual code $\mathscr{C}_{\text{pub}}^{\perp}$ that has for generator matrix $\mathbf{H}_{\text{pub}}$ has codewords of weight $\leq d+t$ since rows of $\mathbf{H}'\mathbf{P}$ belong to this code, and all of its rows have rank weight $\leq d+t$ since the rows of $\mathbf{H}'$ have weight at most $d+t$ and $\mathbf{P}$ is an isometry for the rank metric. The authors have chosen the parameters of the RankSign scheme so that finding codewords of weight $t+d$ in $\mathscr{C}_{\text{pub}}^{\perp}$ is above the security level of the scheme. However, it turns out that due to the peculiar parameters chosen in the RankSign scheme (see Fact 1), $\mathscr{C}_{\text{pub}}$ has many very low weight codewords. This is the main problem in RankSign. Before we give a precise statement together with its proof, we will give a general result showing that LRPC codes may have under certain circumstances low weight codewords.

Lemma 2. *Let $\mathscr{C}$ be an* LRPC *code of length n and dimension k over $\mathbb{F}_{q^m}$ that is associated to an homogeneous matrix $\mathbf{H}$ that has all its entries in a subspace F of $\mathbb{F}_{q^m}$. Furthermore we suppose there exists a subspace F' of $\mathbb{F}_{q^m}$ such that*

$$(n-k)\dim(F\cdot F') < n\dim F'.$$

Then there exist nonzero codewords in the LRPC *code whose support is included in F'. They are therefore of rank weight at most $\dim F'$. Furthermore this set of codewords, that is*

$$\mathscr{C}' \stackrel{\triangle}{=} \{\mathbf{c}\in\mathscr{C} : c_i \in F',\ \forall i \in [\![1,n]\!]\}$$

forms an $\mathbb{F}_q$ subspace of $\mathbb{F}_{q^m}^n$ that is of dimension $\geq n\dim F' - (n-k)\dim(F\cdot F')$.

Proof. Denote the entry in row i and column j of $\mathbf{H}$ by $H_{i,j}$. A codeword $\mathbf{c}$ of the LRPC code satisfies

$$\forall i \in [\![1,n-k]\!],\quad \sum_{j=1}^{n} H_{i,j}c_j = 0. \tag{8}$$

Looking in addition for a codeword $\mathbf{c}$ that has all its entries in F' and expressing these $n-k$ linear equations over $\mathbb{F}_{q^m}$ in a basis of $F\cdot F'$ (since $\sum_{j=1}^{n} H_{i,j}c_j$ belongs by definition to $F\cdot F'$) and expressing each c_j in a $\mathbb{F}_q$ basis $\{f'_1,\ldots,f'_{d'}\}$ of F' as $c_j = \sum_{\ell=1}^{d'} c_{j,\ell}f'_\ell$ we obtain $(n-k)\dim(F\cdot F')$ linear equations over $\mathbb{F}_q$ involving $n\dim F'$ unknowns (the $c_{j,\ell}$'s) in $\mathbb{F}_q$. The solution space is therefore of dimension greater $\geq n\dim F' - (n-k)\dim(F\cdot F')$. □

Remark 4. *This theorem proves the existence of low rank codewords in an LRPC-code under some conditions but it does not give any efficient way to find them.*

By using this lemma, we will prove the following corollary that explains that the augmented LRPC codes that are used in the RankSign signature necessarily contain many rank weight 2 codewords. This is in a sense a consequence of the constraint (4) on the parameters of RankSign.

Corollary 3. *Let $\mathscr{C}_{\text{pub}}$ be an $[n+t,k+t]$ public code of* RankSign *over $\mathbb{F}_{q^m}$ which has been obtained from an $[n,k]$* LRPC*-code that is associated to a homogeneous matrix $\mathbf{H}$ that has all its entries in an $\mathbb{F}_q$ subspace F of $\mathbb{F}_{q^m}$. Consider a subspace F' of F of dimension 2 and let*

$$\mathscr{C}'_{\text{pub}} \stackrel{\triangle}{=} \{\mathbf{c}\in\mathscr{C}_{\text{pub}} : c_i\in F',\ \forall i\in[\![1,n+t]\!]\}.$$

$\mathscr{C}'_{\text{pub}}$ is an $\mathbb{F}_q$ subspace of $\mathbb{F}_{q^m}^{n+t}$. If (4) holds, that is $n=(n-k)d$, then

$$\dim_{\mathbb{F}_q}\mathscr{C}'_{\text{pub}} \geq n/d.$$

Proof. Let $\mathbf{H}_{\text{pub}} \in \mathbb{F}_{q^m}^{(n-k)\times(n+t)}$ be the public parity-check matrix for the RankSign public code $\mathscr{C}_{\text{pub}}$. Recall that $\mathbf{H}_{\text{pub}}$ has been obtained as $\mathbf{H}_{\text{pub}} = \mathbf{Q}\left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}$ where:

- $\mathbf{P}$ is a non-singular matrix with entries in $\mathbb{F}_q$ of size $(n+t)\times(n+t)$,

- $\mathbf{Q}$ is an invertible matrix of $\mathbb{F}_{q^m}$ of size $(n-k)\times(n-k)$,
- $\mathbf{R}$ is a random matrix of $\mathbb{F}_{q^m}$ of size $(n-k)\times t$,
- $\mathbf{H}$ is a homogeneous $(n-k)\times n$ matrix of weight d with all its entries in F.

Choose a basis $\{x_1, x_2, \ldots, x_d\}$ of F such that $\{x_1, x_2\}$ is a basis of F'. We observe now that

$$F \cdot F' = \langle x_i x_j : i \in [\![1,d]\!],\ j \in [\![1,2]\!] \rangle_{\mathbb{F}_q}.$$

The cardinality of the set $\{x_i x_j : i \in [\![1,d]\!],\ j \in [\![1,2]\!]\}$ is actually $2d-1$ because $x_1x_2 = x_2x_1$. This implies that

$$\dim(F \cdot F') \leq 2d-1.$$

It leads to the following inequalities,

$$\begin{aligned} n\dim(F') - (n-k)\dim(F\cdot F') &\geq 2n - (n-k)(2d-1) \\ &= 2d(n-k) - (n-k)(2d-1) \text{ (since } n=(n-k)d) \\ &= n-k \\ &= \frac{n}{d} \quad \text{(since } n=(n-k)d). \end{aligned}$$

Let $\mathscr{C}_{\mathrm{LRPC}}$ be the LRPC code of weight d associated to the parity-check matrix $\mathbf{H}$ and let $\mathscr{C}'_{\mathrm{LRPC}}$ be an $\mathbb{F}_q$ subspace of it that is defined by

$$\mathscr{C}'_{\mathrm{LRPC}} \stackrel{\triangle}{=} \{\mathbf{c} \in \mathscr{C}_{\mathrm{LRPC}} : c_i \in F',\ \forall i \in [\![1,n]\!]\}.$$

By applying Lemma 2 we know that

$$\dim_{\mathbb{F}_q} \mathscr{C}'_{\mathrm{LRPC}} \geq \frac{n}{d}. \tag{9}$$

Consider now

$$\mathscr{C}'_{\mathrm{pub}} \stackrel{\triangle}{=} \{(\mathbf{c}_{\mathrm{LRPC}}, \mathbf{0}_t)(\mathbf{P}^{-1})^{\intercal} : \mathbf{c}_{\mathrm{LRPC}} \in \mathscr{C}'_{\mathrm{LRPC}}\},$$

where $\mathbf{0}_t$ denotes the vector with t zeros. From (9) we deduce that

$$\dim_{\mathbb{F}_q} \mathscr{C}'_{\mathrm{pub}} \geq \frac{n}{d}.$$

Moreover the entries of any element $\mathbf{c}'$ in $\mathscr{C}'_{\mathrm{pub}}$ belong to F' because the entries of $\mathbf{P}$ are in $\mathbb{F}_q$. Let us now prove that $\mathscr{C}'_{\mathrm{pub}}$ is contained in $\mathscr{C}_{\mathrm{pub}}$. To verify this, consider an element $\mathbf{c}'$ in $\mathscr{C}'_{\mathrm{pub}}$. It can be written as

$$\mathbf{c}' = (\mathbf{c}_{\mathrm{LRPC}}, \mathbf{0}_t)(\mathbf{P}^{-1})^{\intercal}.$$

We observe now that

$$\begin{aligned} \mathbf{H}_{\mathrm{pub}}\mathbf{c}'^{\intercal} &= \mathbf{H}_{\mathrm{pub}}\mathbf{P}^{-1}(\mathbf{c}_{\mathrm{LRPC}}, \mathbf{0}_t)^{\intercal} \\ &= \mathbf{Q}\left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}\mathbf{P}^{-1}(\mathbf{c}_{\mathrm{LRPC}}, \mathbf{0}_t)^{\intercal} \\ &= \mathbf{Q}\left[\mathbf{H}|\mathbf{R}\right](\mathbf{c}_{\mathrm{LRPC}}, \mathbf{0}_t)^{\intercal} \\ &= \mathbf{Q}\mathbf{H}\mathbf{c}_{\mathrm{LRPC}}{}^{\intercal} \quad (\ \mathbf{R} \in \mathbb{F}_{q^m}^{(n-k)\times t}\ ) \\ &= \mathbf{0} \quad (\mathbf{c}_{\mathrm{LRPC}} \text{ belongs to the code of parity-check matrix } \mathbf{H}) \end{aligned}$$

This proves that $\mathscr{C}'_{\mathrm{pub}} \subset \mathscr{C}_{\mathrm{pub}}$ which concludes the proof. □

5.2 Weight 1 codewords in a projected code

Corollary 3 shows that there are many weight 2 codewords in $\mathscr{C}_{\text{pub}}$. We can even restrict our search further by noticing that without loss of generality we may assume that the space F in which the entries of the secret parity-check matrix $\mathbf{H}$ of the LRPC code are taken contains 1. Indeed, for any α in $\mathbb{F}_{q^m}^{\times}$, $\alpha\mathbf{H}$ is also a parity-check matrix of the LRPC code and has its entries in αF. By choosing α such that αF contains 1 we get our claim.

Consider now a supplementary space V of $\langle 1\rangle_{\mathbb{F}_q} = \mathbb{F}_q$ with respect to $\mathbb{F}_{q^m}$, that is an $\mathbb{F}_q$-space of dimension $m-1$ such that

$$\mathbb{F}_{q^m} = V \oplus \mathbb{F}_q.$$

The previous discussion implies that there is a matrix-code in $\mathbb{F}_q^{(m-1)\times(n+t)}$, deduced from $\mathscr{C}_{\text{pub}}$ by projecting the entries onto V, that contains codewords of weight 1. More specifically, consider an $\mathbb{F}_q$ basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ of $\mathbb{F}_{q^m}$ such that $\beta_m = 1$ and for $\mathbf{c} = (c_i)_{1\le i\le n+t} \in \mathbb{F}_{q^m}^{n+t}$ consider

$$\mathbf{Mat}^{\text{proj}}(\mathbf{c}) = (M_{ij})_{\substack{1\le i\le m-1\\ 1\le j\le n+t}} \in \mathbb{F}_q^{(m-1)\times(n+t)}$$

where $c_j = \sum_{i=1}^{m} M_{ij}\beta_i$. Now let $\mathscr{C}_{\text{pub}}^{\text{proj}}$ be the matrix-code in $\mathbb{F}_q^{(m-1)\times(n+t)}$ defined by

$$\mathscr{C}_{\text{pub}}^{\text{proj}} \stackrel{\triangle}{=} \left\{\mathbf{Mat}^{\text{proj}}(\mathbf{c})\right\}.$$

It is clear that

Fact 2. *$\mathscr{C}_{\text{pub}}^{\text{proj}}$ contains codewords of rank weight 1.*

These are just the codewords $\mathbf{c}'$ which are of the form $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$ where $\mathbf{c} \in \mathscr{C}'_{\text{pub}}$ with $\mathscr{C}'_{\text{pub}}$ being defined from a subspace F' of F that contains 1 (we can make this assumption since we can assume that F contains 1).

$\mathscr{C}_{\text{pub}}^{\text{proj}}$ has the structure of an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{(m-1)\times(n+t)}$. It is typically of dimension $(k+t)m$ (i.e. the same as the $\mathbb{F}_q$ dimension of $\mathscr{C}_{\text{pub}}$). Moreover once we have these rank weight 1 codewords in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ we can lift them to obtain rank weight ≤ 2 codewords in $\mathscr{C}_{\text{pub}}$ because for any $\mathbf{c} \in \mathscr{C}_{\text{pub}}$ the last row of $\mathbf{Mat}(\mathbf{c})$ can be uniquely recovered from $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$ by performing linear combinations of the entries of $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$. We call this operation deducing $\mathbf{c}$ from $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$ *lifting* from $\mathscr{C}_{\text{pub}}^{\text{proj}}$ to $\mathscr{C}_{\text{pub}}$.

5.3 Outline of the attack

Finding codewords of rank 1 in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ obviously reveals much of the secret LRPC structure. Lifting elements in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ that are of rank 1 to $\mathscr{C}_{\text{pub}}$ as explained at the end of Subsection 5.2 yields codewords of $\mathscr{C}_{\text{pub}}$ that have typically rank weight 2. This can be used to reveal F' and actually the whole subspace F by finding enough rank 1 codewords in $\mathscr{C}_{\text{pub}}^{\text{proj}}$. Once F is recovered a suitable form for a parity-check matrix of $\mathscr{C}_{\text{pub}}$ can be found that allows signing like a legitimate user. For the case of the parameters of RankSign proposed in [GRSZ14, AGH$^+$17] for which we always have $d = 2$ we will proceed slightly differently here. Roughly speaking, our attack can be decomposed as follows

1. We find a particular element $\mathbf{M}$ in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ of rank weight 1 by solving a certain bilinear system with Gröbner bases techniques.

2. We lift $\mathbf{M} \in \mathscr{C}_{\text{pub}}^{\text{proj}}$ to $\mathbf{c} \in \mathscr{C}_{\text{pub}}$ and compute $F' \stackrel{\triangle}{=} \text{Supp}(\mathbf{c})$.

3. We compute from F' the $\mathbb{F}_q$-subspace
   $\mathscr{C}'_{\text{pub}} \stackrel{\triangle}{=} \{\mathbf{c} = (c_i)_{1\le i\le n+t} \in \mathscr{C}_{\text{pub}} : c_i \in F' \ \forall i \in [\![1, n+t]\!]\}$. When $d = 2$ this set has typically dimension k.

4. We use this subspace of $\mathscr{C}_{\mathrm{pub}}$ to find a suitable parity-check matrix for $\mathscr{C}_{\mathrm{pub}}$ which allows us to sign like a legitimate user.

Steps 2. and 3. are straightforward. We just give details for Steps 1. and 4. in what follows.

5.4 Finding rank 1 matrices in $\mathscr{C}_{\mathbf{pub}}^{\mathbf{proj}}$ by solving a bilinear system

The basic bilinear system. Finding rank 1 matrices in $\mathscr{C}_{\mathrm{pub}}^{\mathrm{proj}}$ can be formulated as an instance of the MinRank problem [BFS99, Cou01]. We could use standard techniques for solving this problem [KS99, FLdVP08, FDS10, Spa12] but we found that it is better here to use the algebraic modeling suggested in [AGH+17]. It basically consists in setting up an algebraic system with unknowns $\mathbf{x} = (x_1, \ldots, x_{m-1}) \in \mathbb{F}_q^{m-1}$ and $\mathbf{y} \in \mathbb{F}_q^{n+t}$ where the unknown matrix $\mathbf{M}$ in $\mathscr{C}_{\mathrm{pub}}^{\mathrm{proj}}$ that should be of rank 1 has the form

$$\mathbf{M} = \begin{pmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_{n+t} \\ x_2y_1 & x_2y_2 & \cdots & x_2y_{n+t} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m-1}y_1 & x_{m-1}y_2 & \cdots & x_{m-1}y_{n+t} \end{pmatrix}.$$

Recall that $\mathscr{C}_{\mathrm{pub}}^{\mathrm{proj}}$ has the structure of an $\mathbb{F}_q$ subspace of $\mathbb{F}_q^{(m-1)\times(n+t)}$ of dimension $(k+t)m$. By viewing the elements of $\mathscr{C}_{\mathrm{pub}}^{\mathrm{proj}}$ as vectors of $\mathbb{F}_q^{(m-1)(n+t)}$, i.e. the matrix $\mathbf{M} = (M_{ij})_{\substack{1\le i\le m-1\\ 1\le j\le n+t}}$ is viewed as the vector $\mathbf{m} = (m_\ell)_{1\le \ell\le (m-1)(n+t)}$ where $m_{(i-1)(n+t)+j} = M_{i,j}$, we can compute a parity-check matrix $\mathbf{H}_{\mathrm{pub}}^{\mathrm{proj}}$ for it. It is an $((m-1)(n+t)-(k+t)m) \times (m-1)(n+t)$ matrix that we denote by $\mathbf{H}_{\mathrm{pub}}^{\mathrm{proj}} = (H_{ij}^{\mathrm{proj}})_{\substack{1\le i\le (m-1)(n+t)-(k+t)m\\ 1\le j\le (m-1)(n+t)}}$. This matrix gives $(m-1)(n+t)-(k+t)m$ bilinear equations that have to be satisfied by the x_i's and the y_j's:

$$\begin{cases} \sum_{j=1}^{n+t}\sum_{i=1}^{m-1} H_{1,(i-1)(n+t)+j}^{\mathrm{proj}} x_i y_j = 0 \\ \qquad \vdots \\ \sum_{j=1}^{n+t}\sum_{i=1}^{m-1} H_{(n+t)(m-1)-(k+t)m,(i-1)(n+t)+j}^{\mathrm{proj}} x_i y_j = 0 \end{cases} \tag{10}$$

Restricting the number of solutions. We have solved the bilinear system (10) with standard Gröbner bases techniques that are implemented in Magma. To speed-up the resolution of the bilinear system with Gröbner bases techniques (especially the change of order that is performed after a first computation of a Gröbner basis for a suitable order to deduce a basis for the lexicographic order which is more suited for outputting a solution) it is helpful to use additional equations that restrict the solution space which is otherwise really huge in this case. The purpose of the following discussion is to show where these solutions come from and how to restrict them. By bilinearity of System (10) we may fix

$$x_1 = 1 \tag{11}$$

when there is a solution $\mathbf{x}$ such that $x_1 \neq 0$). Furthermore, the fact that $\mathscr{C}'_{\mathrm{pub}}$ is an $\mathbb{F}_q$ vector space of dimension n/d induces that for a given $\mathbf{x}$ solution to (10) the set of corresponding $\mathbf{y}$'s also forms a vector space of dimension n/d. We may therefore rather safely assume that we can choose

$$\forall i \in [\![1, \frac{n}{d} - 1]\!],\ y_i = 0 \quad \text{and} \quad y_{n/d} = 1. \tag{12}$$

There is an additional degree of freedom on $\mathbf{x}$ coming from the fact that even if $d = 2$ there are several spaces αF for which $1 \in \alpha F$. To verify this, let us study in more detail the case when F is of dimension 2, say

$$F = \langle a, b \rangle_{\mathbb{F}_q}.$$

Intended Security [AGH+17]	(n, k, m, d, t, q)	Time	Maximum Memory Usage
128 bits	$(20, 10, 21, 2, 2, 2^{32})$	20.12 s	49 MB
128 bits	$(24, 12, 24, 2, 2, 2^{24})$	31.75 s	65 MB
192 bits	$(24, 12, 27, 2, 3, 2^{32})$	125.64 s	97 MB
256 bits	$(28, 14, 30, 2, 3, 2^{32})$	256.90 s	137 MB

Table 1: Attack on NIST's parameters of RankSign

We wish to understand what are the possible values for $z \in \mathbb{F}_{q^m}$ such that there exists $c \neq 0$ for which

$$\langle a, b\rangle_{\mathbb{F}_q} = c\langle 1, z\rangle_{\mathbb{F}_q}.$$

The possible values for $\mathbf{x}$ will then be the projection of those z to the $\mathbb{F}_q$ space $\langle \beta_1, \ldots, \beta_{m-1}\rangle_{\mathbb{F}_q}$. The possible values for z are then obtained from studying the possible values for c. There are two cases to consider:

- **Case 1:** $c = \frac{\mu}{a+b\nu}$ for $\mu \in \mathbb{F}_q^\times$ and $\nu \in \mathbb{F}_q$. In such a case

$$z = \frac{\beta b}{a + b\nu} + \delta$$

  for $\beta \in \mathbb{F}_q^\times$, $\delta \in \mathbb{F}_q$.

- **Case 2:** $c = \frac{\mu}{b}$ for $\mu \in \mathbb{F}_q^\times$. Here

$$z = \alpha\frac{a}{b} + \delta$$

  for $\alpha \in \mathbb{F}_q^\times$, $\delta \in \mathbb{F}_q$.

Since the δ term vanishes after projecting x onto $\langle \beta_1, \ldots, \beta_{m-1}\rangle_{\mathbb{F}_q}$ we have essentially two degrees of freedom over $\mathbb{F}_q$ for x. One has already been taken into account when setting $x_1 = 1$. We can add a second one $x_2 = \alpha$ where α is arbitrary in $\mathbb{F}_q$. We have actually chosen in our experiments that

$$(x_2 - \alpha)(x_2 - \beta) = 0 \tag{13}$$

for some random α and β in $\mathbb{F}_q$. This has resulted in some gain in the computation of the solution space. Finally the following proposition summarizes the system we have solved.

Proposition 4. *By eliminating variables using Equations* (11),(12) *and* (13) *in* (10) *we have*

- $nm - k(m+1) - t + 2$ *equations;*
- $m - 1 + n + t$ *unknowns.*

In the "typical regime" where $m \approx n$, $k \approx \frac{n}{2}$ and $t \ll n$ we have a number of equations of order n^2 and a number of unknowns of order n, therefore typically the regime where we expect that the Gröbner basis techniques take polynomial time.

5.5 Numerical results

We give in Table 1 our numerical results to find a codeword of rank 2 in any public code of the RankSign scheme for parameters chosen according to [AGH+17]. These results have been obtained with an Intel Core i5 processor, clocked at 1.6 GHz using a single core, with 8 Go of RAM.

5.6 Finishing the attack

We present in this subsection the end of our attack which consists in being able to sign with only the knowledge of the public key. It holds for the parameters chosen for the NIST competition [AGH+17] for which $d = 2$. Observe that (4) implies that we have $k = n - k = n/2$.

We have at that point obtained the code $\mathscr{C}'_{\rm pub}$ (see §5.3, Point 3.) that has dimension (over $\mathbb{F}_q$) $\geq n/d = n/2 = k$. This code is just $\mathbb{F}_q$-linear, but it will be convenient to extend it by considering its $\mathbb{F}_{q^m}$-linear extension, that we denote $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}$ that is defined by the $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^{n+t}$ obtained from linear combinations over $\mathbb{F}_{q^m}$ of codewords in $\mathscr{C}'_{\rm pub}$. In other words if we denote by $\{\mathbf{c}'_1, \ldots, \mathbf{c}'_{k'}\}$ an $\mathbb{F}_q$-basis of $\mathscr{C}'_{\rm pub}$, then

$$\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub} = \langle \mathbf{c}'_1, \ldots, \mathbf{c}'_{k'} \rangle_{\mathbb{F}_{q^m}}.$$

To simplify the discussion we make now the following assumption (which was corroborated by our experiments)

Assumption 1.

$$\dim \mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub} = k.$$

The rationale behind this assumption is that (i) the dimension of $\mathscr{C}'_{\rm pub}$ is very likely to be n/d which is equal to k and (ii) an $\mathbb{F}_q$ basis of $\mathscr{C}'_{\rm pub}$ is very likely to be an $\mathbb{F}_{q^m}$ basis too.

Lemma 5. *Under Assumption 1 the code* $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}\right)^\perp$ *has length* $n + t$*, dimension* $n + t - k$ *and is an* LRPC*-code that is associated to a homogeneous matrix that has all its entries in an* $\mathbb{F}_q$ *subspace* F *of* $\mathbb{F}_{q^m}$ *of dimension* 2 *which contains* 1*. Furthermore, the sets*

$$\mathscr{D} \stackrel{\triangle}{=} \{\mathbf{c} \in \left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}\right)^\perp : \mathrm{Supp}(\mathbf{c}) \subseteq \mathbb{F}_q\} \text{ and } \mathscr{D}' \stackrel{\triangle}{=} \{\mathbf{c} \in \left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}\right)^\perp : \mathrm{Supp}(\mathbf{c}) \subseteq F\}$$

are $\mathbb{F}_q$*-subspaces of dimension* $\geq t$ *and* $\geq n - k + 2t$ *respectively.*

Proof. By Assumption 1, $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}$ is of dimension k and its dual $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}\right)^\perp$ has therefore dimension $n + t - k$. There is a generator matrix for $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}$ that is formed by rows taken from $\mathscr{C}'_{\rm pub}$. It is homogeneous of weight 2. Say that its entries generate a space F. This is also a parity-check matrix of the dual code. $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}\right)^\perp$ is therefore an LRPC code of weight 2.

By applying now Lemma 2 to it with $F' = \mathbb{F}_q$, we have

$$\begin{aligned}(n+t)\dim_{\mathbb{F}_q}(\mathbb{F}_q) - (n+t-(n+t-k))\dim(F\cdot\mathbb{F}_q) &= n+t-2k\\ &= t \text{ (because } 2k = n)\end{aligned}$$

which gives the result for the set $\mathscr{D}$. We apply once again Lemma 2 but this time with $F' = F$. Say $F = \langle 1, x_1 \rangle_{\mathbb{F}_q}$. This gives a lower bound on the dimension of $\mathscr{D}'$ which is

$$\begin{aligned}(n+t)\dim(F) - (n+t-(n+t-k))\dim(F\cdot F) &\geq 2(n+t) - 3k\\ &\text{(because } F\cdot F = \langle 1, x_1, x_1^2\rangle_{\mathbb{F}_q})\\ &= n-k+2t \text{ (because } 2k = n).\end{aligned}$$

□

To end our attack we make now the following assumption that was again corroborated in our experiments.

Assumption 2. *We can extract from sets* $\mathscr{D}$ *and* $\mathscr{D}'$ *a basis of* $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\rm pub}\right)^\perp$ *with*

1. t *codewords of support* $\mathbb{F}_q$*,*

2. $n-k$ *codewords of a same support of rank* 2 *which contains* 1.

Lemma 6. *Under Assumptions 1 and 2 there exists a parity-check matrix* $\mathbf{H}' \in \mathbb{F}_{q^m}^{(n+t-k)\times(n+t)}$ *of* $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$*, an invertible matrix* $\mathbf{P}$ *of size* $n+t$ *with entries in the small field* $\mathbb{F}_q$ *and an invertible matrix* $\mathbf{S}$ *of size* $n+t-k$ *with entries in* $\mathbb{F}_{q^m}$ *such that*

$$\mathbf{SH}'\mathbf{P} = \begin{pmatrix} I_t & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

where $\mathbf{R}$ *is homogeneous of degree* 2 *and of size* $(n-k)\times n$*.*

Proof. Under Assumptions 1 and 2 there is a generator matrix of $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp}$ and thus a parity-check matrix of $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$ which is homogeneous of degree 2 with the particularity that t rows of it are of rank 1. Let $\mathbf{H}'$ be such a matrix, thus by making a Gaussian elimination on its rows we have an invertible matrix $\mathbf{S} \in \mathbb{F}_{q^m}^{(n+t-k)\times(n+t-k)}$ such that:

$$\mathbf{SH}' = \begin{pmatrix} I_t & \mathbf{Q} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

where $\mathbf{Q}$ is a matrix of size $t\times(n+t)$ whose entries lie in the small field $\mathbb{F}_q$ and $\mathbf{R}$ is a homogeneous matrix of weight 2 and of size $(n-k)\times n$. In this way there exists an invertible matrix $\mathbf{P}$ of size $(n+t)\times(n+t)$ with coefficients in the field $\mathbb{F}_q$ such that

$$\mathbf{SH}'\mathbf{P} = \begin{pmatrix} I_t & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

which concludes the proof. □

The idea now to sign as a legitimate user will be to use the matrix $\mathbf{R}$ and the decoder of Fact 1 (see Section §3). Recall that to make a signature for the matrix $\mathbf{H}_{\text{pub}}$ (which defines the public code $\mathscr{C}_{\text{pub}}$) and a message $\mathbf{m}$, we look for an error $\mathbf{e}$ of rank w satisfying $n-k = d(w-t-t')$ (see Equation (3) of Fact 1), such that $\mathbf{H}_{\text{pub}}\mathbf{e}^{\intercal} = \mathbf{s}^{\intercal}$ with $\mathbf{s} = \mathscr{H}(\mathbf{m})$ (the hash of the message). The algorithm that follows performs this task:

1. We compute $\mathbf{y} \in \mathbb{F}_{q^m}^{n+t}$ such that $\mathbf{H}_{\text{pub}}\mathbf{y}^{\intercal} = \mathbf{s}^{\intercal}$.
2. Let $\mathbf{y}' = \mathbf{y}(\mathbf{P}^{-1})^{\intercal}$ and we compute $\mathbf{s}' = (\mathbf{SH}'\mathbf{P})\mathbf{y}'^{\intercal}$.
3. Let $\mathbf{s}'_1$ be the first t coordinates of $\mathbf{s}'$, $\mathbf{s}'_2$ its last $n-k$ ones. We apply the decoder of §3 with:

   - The subspace $T \stackrel{\triangle}{=} \text{Supp}(\mathbf{s}'_1) + T'$ where T' is a random subspace of $\mathbb{F}_{q^m}$ of dimension t'.

   - The parity-check matrix $\mathbf{R}$ and the syndrome $\mathbf{s}'_2$.

   Then we get a vector $\mathbf{e}'$ such that $T \subseteq \text{Supp}(\mathbf{e}')$ and $\mathbf{R}\mathbf{e}'^{\intercal} = \mathbf{s}'^{\intercal}_2$.
4. We compute $\mathbf{e} = (\mathbf{s}'_1, \mathbf{e}')\mathbf{P}^{\intercal}$.

Let us now show the correctness of this algorithm, in other words we show that $\mathbf{H}_{\text{pub}}\mathbf{e}^{\intercal} = \mathbf{s}^{\intercal}$ with $|\mathbf{e}| = w$ satisfying $n-k = 2(w-t-t')$.

Proof of Correctness. First we have:

$$\begin{aligned}
\mathbf{H}'\mathbf{e}^\intercal &= \mathbf{H}'\mathbf{P}(\mathbf{s}'_1, \mathbf{e}')^\intercal \\
&= \mathbf{S}^{-1}(\mathbf{S}\mathbf{H}'\mathbf{P})(\mathbf{s}'_1, \mathbf{e}')^\intercal \\
&= \mathbf{S}^{-1}\begin{pmatrix} I_t & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}(\mathbf{s}'_1, \mathbf{e}')^\intercal \\
&= \mathbf{S}^{-1}\begin{pmatrix} \mathbf{s}_1'^\intercal \\ \mathbf{R}\mathbf{e}'^\intercal \end{pmatrix} \text{ (because } \mathbf{s}'_1 \text{ of size } t) \\
&= \mathbf{S}^{-1}\mathbf{s}'^\intercal \text{ (because } \mathbf{R}\mathbf{e}'^\intercal = \mathbf{s}_2'^\intercal) \\
&= \mathbf{S}^{-1}(\mathbf{S}\mathbf{H}'\mathbf{P})\mathbf{y}'^\intercal \\
&= \mathbf{H}'\mathbf{P}(\mathbf{P}^{-1}\mathbf{y}^\intercal) \\
&= \mathbf{H}'\mathbf{y}^\intercal
\end{aligned}$$

which implies that $\mathbf{H}'(\mathbf{e}-\mathbf{y})^\intercal = \mathbf{0}$ and $\mathbf{y}-\mathbf{e} \in \mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$. Recall now that $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}} \subseteq \mathscr{C}_{\text{pub}}$ and therefore $\mathbf{H}_{\text{pub}}(\mathbf{e}-\mathbf{y})^\intercal = \mathbf{0}$. By linearity we get $\mathbf{H}_{\text{pub}}\mathbf{e}^\intercal = \mathbf{H}_{\text{pub}}\mathbf{y}^\intercal = \mathbf{s}^\intercal$.
Thus under the condition that the decoder in Point 3 works for the matrix $\mathbf{H}'$, the syndrome $\mathbf{s}$ and the subspace T, our algorithm decodes the syndrome $\mathbf{s}$ relatively to $\mathbf{H}_{\text{pub}}$.
The parity-check matrix $\mathbf{R}$ is homogeneous of degree 2, has $n-k$ rows and n columns. We can therefore apply to it the decoder of §3. It will output (we use here Fact 1) an error $\mathbf{e}'$ of weight w' that satisfies $n-k = 2(w'-t-t')$. Note that this implies that $w' = w$ which is the error weight we want to achieve. Then the error $\mathbf{e} = (\mathbf{s}'_1, \mathbf{e}')\mathbf{P}^\intercal$ has the same rank as $\text{Supp}(\mathbf{s}'_1) \subseteq T \subseteq \text{Supp}(\mathbf{e}')$ and $\mathbf{P}$ is an invertible matrix in the small field which concludes the proof.

□

6 Attack on the IBE in the rank metric

In the previous section we showed that RankSign is not a secure signature scheme. This also shows the insecurity of the IBE proposal made in [GHPT17] since it is partly based on it. It could be thought that it just suffices to replace in the IBE scheme [GHPT17] RankSign by another signature scheme in the rank metric. This is already problematic, since RankSign was the only known rank metric code-based signature scheme up to now. We will actually show here that the problem is deeper than this. We namely show that the parameters proposed in [GHPT17] can be broken by an algebraic attack that attacks the RSL problem directly and not the underlying signature scheme. We will however show that the constraints on the parameters of the scheme coming from Proposition 1 together with the new constraint for avoiding the algebraic attack exposed here can in theory be met. In the IBE [GHPT17] we are given a matrix $\mathbf{G}_{\mathscr{C}_{\text{sgn}}}$ of size $k_{\text{sgn}} \times n_{\text{sgn}}$ whose coefficients live in $\mathbb{F}_{q^m}$ and the matrix $\mathbf{G}_{\mathscr{C}_{\text{sgn}}}\mathbf{E}$ where $\mathbf{E}$ has size $n_{\text{sgn}} \times N_{\text{dec}}$ with all its coefficients which live in a same secret subspace F of dimension d and an attacker wants to recover F. We show in §6.1 that under the condition $N_{\text{dec}} > d(n_{\text{sgn}} - k_{\text{sgn}})$ (which is verified in [GHPT17]) the code $\mathscr{C}$ defined by

$$\mathscr{C} = \{\mathbf{e}(\mathbf{G}_{\text{sgn}}\mathbf{E})^\intercal : \mathbf{e} \in \mathbb{F}_q^{N_{\text{dec}}}\} \subseteq \mathbb{F}_{q^m}^{k_{\text{sgn}}}. \tag{14}$$

is an $\mathbb{F}_q$-subspace which contains words of weight $\leq d$ which reveal F. It turns out that the subspace $\mathscr{C}' \triangleq \mathscr{C} \cap F^{N_{\text{dec}}}$ of words of $\mathscr{C}$ whose coordinates all live in F is of dimension $\geq N_{\text{dec}} - d(n_{\text{sgn}} - k_{\text{sgn}})$. We then apply standard algebraic techniques in Subsection §6.2 to recover $\mathscr{C}'$ and therefore F from it. This breaks all the parameters proposed in [GHPT17]. We conclude this section by showing that there is in principle a way to choose the parameters of the IBE scheme to possibly avoid this attack.

6.1 Low rank codewords from instances of the RSL problem

We prove here that a certain $\mathbb{F}_q$-linear code that contains many low-weight codewords can be computed by the attacker. This is explained by

Theorem 1. *Let* $(\mathbf{A}, \mathbf{AE})$ *be an instance of* RSL *for parameters* n, k, N, d *with* $\mathbf{A} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ *in systematic form and* $\mathbf{E} \in \mathbb{F}_{q^m}^{n\times N}$ *where all its coefficients belong to a same subspace* F *of dimension* d*. Furthermore, we suppose that*

$$N > dk. \tag{15}$$

Let

$$\begin{aligned} \mathscr{C} &\stackrel{\triangle}{=} \{\mathbf{e}(\mathbf{AE})^\intercal : \mathbf{e} \in \mathbb{F}_q^N\} \\ \mathscr{C}' &\stackrel{\triangle}{=} \mathscr{C} \cap F^{n-k}. \end{aligned}$$

$\mathscr{C}'$ *is an* $\mathbb{F}_q$*-subspace of* $\mathscr{C}$ *of dimension* $\geq N - dk$*.*

Proof. Let us first decompose $\mathbf{E}$ in two parts $\left[\frac{\mathbf{E}_1}{\mathbf{E}_2}\right]$ where $\mathbf{E}_1$ is formed by the first $n-k$ rows of $\mathbf{E}$ and $\mathbf{E}_2$ by the last k ones. The matrix $\mathbf{A}$ is in systematic form, namely $(I_{n-k}|\mathbf{A}')$ where $\mathbf{A}' \in \mathbb{F}_{q^m}^{(n-k)\times k}$, which gives:

$$\mathbf{AE} = \mathbf{E}_1 + \mathbf{A}'\mathbf{E}_2$$

Therefore, to prove our theorem we just need to show that

$$\mathscr{S} \stackrel{\triangle}{=} \{\mathbf{e} \in \mathbb{F}_q^N : \mathbf{E}_2\mathbf{e}^\intercal = \mathbf{0}\}$$

is an $\mathbb{F}_q$-subspace of dimension greater than $N - dk$. Indeed, for each error $\mathbf{e}$ of $\mathscr{S}$ we have $(\mathbf{AE})\mathbf{e}^\intercal = \mathbf{E}_1\mathbf{e}^\intercal$ which belongs to F^{n-k} as coefficients of $\mathbf{E}_1$ are in the $\mathbb{F}_q$-subspace F and those of $\mathbf{e}$ are in $\mathbb{F}_q$.
Denote the entry in row i and column j of $\mathbf{E}_2$ by $E_{i,j}$. A word of $\mathscr{S}$ satisfies

$$\forall i \in [\![1, k]\!], \quad \sum_{j=1}^{N} E_{i,j}e_j = 0.$$

Looking in addition for $\mathbf{e}$ that has all its entries in $\mathbb{F}_q$ and expressing these k linear equations over $\mathbb{F}_{q^m}$ in a basis of F (since $\sum_{j=1}^N E_{i,j}e_j$ belongs by definition to $F\cdot\mathbb{F}_q = F$) we obtain $k\dim(F) = kd$ linear equations over $\mathbb{F}_q$ involving N unknowns (the e_j's) in $\mathbb{F}_q$. The solution space is therefore of dimension greater than $N - dk$ which concludes the proof of the theorem. □

6.2 How to find low rank codewords in instances of the RSL problem

Theorem 1 showed that there are many codewords of weight $\leq d$ in the code $\mathscr{C}$ defined in (14). Let us show now how these codewords can be recovered by an algebraic attack. The sufficient condition $N_{\text{dec}} > d(n_{\text{sgn}} - k_{\text{sgn}})$ ensuring the existence of such codewords is met for the parameters proposed in [GHPT17].

To explain our algebraic modeling of the problem, let us first recall that for a fixed basis $(\beta_1, \cdots, \beta_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ we can view elements of $\mathbb{F}_{q^m}^{k_{\text{sgn}}}$ as matrices of size $m \times k_{\text{sgn}}$:

$$\forall \mathbf{x} \in \mathbb{F}_{q^m}^{k_{\text{sgn}}}, \quad \mathbf{Mat}(\mathbf{x}) = (X_{i,j}) \in \mathbb{F}_q^{m\times k_{\text{sgn}}} \text{ where } x_j = \sum_{i=1}^{m} \beta_i X_{i,j}.$$

The associated matrix code $\mathscr{C}^{\text{Mat}}$ is defined as:

$$\mathscr{C}^{\text{Mat}} \stackrel{\triangle}{=} \{\mathbf{Mat}(\mathbf{c}) : \mathbf{c} \in \mathscr{C}\} \subseteq \mathbb{F}_q^{m\times k_{\text{sgn}}}.$$

It is easily verified that this matrix-code has dimension N_{dec}. It is clear now by applying Theorem 1 that:

Fact 3. $\mathscr{C}^{\mathrm{Mat}}$ contains codewords of rank $\leq \dim(F)$ which form a $\mathbb{F}_q$-subspace of dimension $\geq N_{\mathrm{dec}} - d(n_{\mathrm{sgn}} - k_{\mathrm{sgn}})$.

These are just the codewords $\mathbf{c}'$ which are of the form $\mathbf{Mat}(\mathbf{c})$ where $\mathbf{c} \in \mathscr{C}$ with $\mathrm{Supp}(\mathbf{c}) \subseteq F$. We do not expect other codewords of this rank in $\mathscr{C}^{\mathrm{Mat}}$ since d is much smaller than the Varshamov-Gilbert bound in the case of the parameters proposed in [GHPT17].

The basic bilinear system. Finding codewords of rank d in $\mathscr{C}^{\mathrm{Mat}}$ can be expressed as an instance of the MinRank problem [BFS99, Cou01]. Once again we propose the algebraic modeling which was suggested in [AGH+17]. It consists here in setting up the algebraic system with unknowns $\mathbf{x}^i = (x_1^i, \cdots, x_m^i) \in \mathbb{F}_q^m$ and $\mathbf{y}_j^i \in \mathbb{F}_q^{k_{\mathrm{sgn}}}$ for $1 \leq i \leq d$ and $1 \leq j \leq k_{\mathrm{sgn}}$ where the $\mathbf{x}^i$'s can be thought as a basis of the unknown subspace F and the $\mathbf{y}_j^i$'s as coordinates of the codeword in this basis. In that case the codeword $\mathbf{M}$ of $\mathscr{C}^{\mathrm{Mat}}$ of rank d has the following form:

$$\mathbf{M} = \begin{pmatrix} \sum_{i=1}^d x_1^i y_1^i & \sum_{i=1}^d x_1^i y_2^i & \cdots & \sum_{i=1}^d x_1^i y_{k_{\mathrm{sgn}}}^i \\ \sum_{i=1}^d x_2^i y_1^i & \sum_{i=1}^d x_2^i y_2^i & \cdots & \sum_{i=1}^d x_2^i y_{k_{\mathrm{sgn}}}^i \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{i=1}^d x_m^i y_1^i & \sum_{i=1}^d x_m^i y_2^i & \cdots & \sum_{i=1}^d x_m^i y_{k_{\mathrm{sgn}}}^i \end{pmatrix}.$$

Recall now that $\mathscr{C}^{\mathrm{Mat}}$ has the structure of an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m \times k_{\mathrm{sgn}}}$ of dimension N. By viewing the elements of $\mathscr{C}^{\mathrm{Mat}}$ as vectors of $\mathbb{F}_q^{mk_{\mathrm{sgn}}}$, i.e. the matrix $\mathbf{M} = (M_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq k_{\mathrm{sgn}}}}$ is viewed as the vector $\mathbf{m} = (m_\ell)_{1 \leq \ell \leq mk_{\mathrm{sgn}}}$ where $m_{(i-1)k_{\mathrm{sgn}}+j} = M_{i,j}$, we can compute a parity-check matrix $\mathbf{H}^{\mathrm{Mat}}$ for it. It is an $(mk_{\mathrm{sgn}} - N_{\mathrm{dec}}) \times mk_{\mathrm{sgn}}$ matrix that we denote by $\mathbf{H}^{\mathrm{Mat}} = (H_{ij}^{\mathrm{Mat}})_{\substack{1 \leq i \leq mk_{\mathrm{sgn}} - N_{\mathrm{dec}} \\ 1 \leq j \leq mk_{\mathrm{sgn}}}}$. This matrix gives $mk_{\mathrm{sgn}} - N_{\mathrm{dec}}$ bilinear equations that have to be satisfied by the x_i^l's and the y_j^l's:

$$\begin{cases} \sum_{l=1}^{d} \sum_{j=1}^{k_{\mathrm{sgn}}} \sum_{i=1}^{m} H_{1,(i-1)k_{\mathrm{sgn}}+j}^{\mathrm{Mat}} x_i^l y_j^l = 0 \\ \qquad \vdots \\ \sum_{l=1}^{d} \sum_{j=1}^{k_{\mathrm{sgn}}} \sum_{i=1}^{m} H_{mk_{\mathrm{sgn}}-N_{\mathrm{dec}},(i-1)k_{\mathrm{sgn}}+j}^{\mathrm{Mat}} x_i^l y_j^l = 0 \end{cases} \tag{16}$$

Restricting the number of solutions. We have solved the bilinear system (16) with Gröbner basis techniques that are implemented in Magma. To speed-up the resolution, as in the case of the attack on RankSign, we add new equations to (16) which come from the vectorial structure of F and the set of solutions.
With our notation we can view F as an $\mathbb{F}_q$ subspace of $\mathbb{F}_q^m$ of dimension d generated by the rows of the matrix:

$$\begin{pmatrix} x_1^1 & \cdots & x_m^1 \\ x_1^2 & \cdots & x_m^2 \\ \vdots & & \vdots \\ x_1^d & \cdots & x_m^d \end{pmatrix}$$

In this way, we can put this matrix into systematic form, it will generate the same subspace. Therefore we can add equations

$$\forall (i,j) \in [\![1,d]\!]^2,\ j \neq i, \quad x_i^j = 0 \text{ and } x_i^i = 1 \tag{17}$$

Intended Security	$(n_{\text{sgn}}, k_{\text{sgn}}, m, d, N_{\text{dec}}, q)$	Time	Maximum Memory Usage
128 bits	$(100, 80, 96, 4, 96, 2^{192})$	626s	1.7 GB

Table 2: Attack on parameters of the rank-based IBE [GHPT17]

without modifying the set of codewords of rank d. Furthermore, this set is an $\mathbb{F}_q$-subspace of dimension greater than $N_{\text{dec}} - (n_{\text{sgn}} - k_{\text{sgn}})d$ and as in the case of the attack on RankSign we may assume that for a random subset $I \subseteq [\![1, k_{\text{sgn}}]\!] \times [\![1, d]\!]$ of size $N_{\text{dec}} - (n_{\text{sgn}} - k_{\text{sgn}}) - 1$ there is an element in this set for which:

$$\forall (j,i) \in I,\ y_j^i = 0 \text{ and } y_{j_0}^{i_0} = 1 \text{ for } (i_0, j_0) \notin I. \tag{18}$$

Equations (17) and (18) enable us to reduce the number of variables of the previous bilinear system. The following proposition summarizes the number of equations and variables that we finally get.

Proposition 7. *By eliminating variables using Equations* (17) *and* (18) *in* (16) *we obtain*

- $mk_{\text{sgn}} + d^2 + (n_{\text{sgn}} - k_{\text{sgn}})$ *equations;*
- $md + k_{\text{sgn}}d$ *unknowns.*

In the "typical regime" where $m \approx n_{\text{sgn}} \approx k_{\text{sgn}}$ and $d \approx n^{\varepsilon}$ for some ε in $(0, 1)$ we have a number of equations of order n^2 and a number of unknowns of order $n^{1+\varepsilon}$, therefore typically the regime where we expect that the Gröbner basis techniques take subexponential time.

6.3 Numerical results

We give in Table 2 our numerical results to find codewords of rank d in instances of the RSL problem for the parameters chosen according to [GHPT17]. These results have been obtained with an Intel Core i5 processor, clocked at 1.6 GHz using a single core, with 8 Go of RAM. In our implementation, we verified that when we generated an instance whose associated secret is the subspace F we only got codewords whose coordinates live in this subspace and therefore revealed it.

6.4 Avoiding the attack

Although our attack breaks the parameters proposed in [GHPT17], there might in principle be a way to instantiate the IBE with a new signature scheme. Recall that the constraints that are to be satisfied are given by

$$w_{\text{rVG}}(q, m, n_{\text{sgn}}, k_{\text{sgn}}) \leq w_{\text{sgn}} \leq \frac{m(n_{\text{sgn}} - k_{\text{sgn}})}{\max(m, n_{\text{sgn}})} \text{ (signature constraint)} \tag{19}$$

$$w_{\text{sgn}}d \leq w_{\text{rVG}}(q, m, N_{\text{dec}}, k_{\text{dec}}) \text{ (decoding works)} \tag{20}$$

$$d(n_{\text{sgn}} - k_{\text{sgn}}) \geq N_{\text{dec}} \text{ (for avoiding our attack).} \tag{21}$$

The lower-bound in (19) ensures that we can find a signature whereas the role of the upper-bound is to ensure that the problem of finding a signature does not become easy. The constraint (20) is here to ensure that the decoding procedure used for recovering the plaintext works and the last constraint is here to avoid our attack. It seems that the set of parameters can be chosen to be non-empty. We first propose to choose $m = n_{\text{sgn}}$ and a signature code for which the ratio $\frac{w_{\text{rVG}}(q,m,n_{\text{sgn}},k_{\text{sgn}})}{n_{\text{sgn}}-k_{\text{sgn}}}$ is sufficiently small (it can even approach $\frac{1}{2}$) and we choose

$$w_{\text{sgn}} = (1 - \varepsilon)(n_{\text{sgn}} - k_{\text{sgn}}) \tag{22}$$

for some appropriate ϵ. We then choose an $\mathbb{F}_{q^m}$-linear code of parameters $[N_{\text{dec}}, k_{\text{dec}}]$ of length $N_{\text{dec}} \gg w_{\text{sgn}}$ and sufficiently small dimension such that

$$w_{\text{rVG}}(q, m, N_{\text{dec}}, k_{\text{dec}}) \geq (1-\varepsilon) N_{\text{dec}}. \tag{23}$$

This is possible in principle. We then choose a d such that (20) holds. By satisfying the two first constraints (19) and (20) in this way, we also satisfy the last one, namely Equation (21). This can be verified by arguing that

$$\begin{aligned} d(n_{\text{sgn}} - k_{\text{sgn}}) &= \frac{w_{\text{sgn}} d}{1-\varepsilon} \quad \text{(we use (22))} \\ &\leq \frac{w_{\text{rVG}}(q, m, N_{\text{dec}}, k_{\text{dec}})}{1-\varepsilon} \quad \text{(we use (20))} \\ &\leq N_{\text{dec}} \quad \text{(we use (23))} \end{aligned}$$

7 Attack on the IBE in the Hamming metric

The purpose of this section is to show that there is an even more fundamental problem with the general IBE scheme given in Section 4 in the Hamming metric. We will namely prove here that due to the constraint on the parameters coming from Proposition 1, we can not find a set of parameters which would avoid an attack based on using generic decoding techniques. Even the simplest of those techniques, namely the Prange algorithm [Pra62], breaks the IBE in the Hamming metric in polynomial time. We refer the reader to Section §4 where we introduced all the notations that we are going to use.

To show that the IBE can be attacked in the Hamming metric we proceed as follows. The attacker knows $\mathbf{G}_{\mathscr{C}_{\text{sgn}}} \mathbf{E}$ and that the columns of $\mathbf{E}$ have weight d. We will show that we can solve efficiently for the range of parameters admissible for the IBE the following syndrome decoding problem: given a matrix $\mathbf{G}_{\mathscr{C}_{\text{sgn}}} \in \mathbb{F}_2^{k_{\text{sgn}} \times n_{\text{sgn}}}$ and $\mathbf{s} \in \mathbb{F}_2^{k_{\text{sgn}}}$ such that there exists $\mathbf{e} \in \mathbb{F}_2^{n_{\text{sgn}}}$ of weight d for which $\mathbf{G}_{\mathscr{C}_{\text{sgn}}} \mathbf{e}^\intercal = \mathbf{s}^\intercal$, we want to recover $\mathbf{e}$. This allows to recover the columns of $\mathbf{E}$ and therefore $\mathbf{E}$. The scheme is broken with this knowledge, since the attacker also knows $\mathscr{H}(id)\mathbf{E} + \mathbf{m}\mathbf{G}_{\mathscr{C}_{\text{dec}}}$, $\mathscr{H}(id)$ and $\mathbf{G}_{\mathscr{C}_{\text{dec}}}$. This is used to derive $\mathbf{m}\mathbf{G}_{\mathscr{C}_{\text{dec}}}$ and finally $\mathbf{m}$.

To solve this decoding problem, we use the Prange algorithm (see [Pra62]) whose complexity is, up to a polynomial factor in n_{sgn}, equal to:

$$\frac{\binom{n_{\text{sgn}}}{d}}{\binom{k_{\text{sgn}}}{d}} \tag{24}$$

In the special case of the IBE we proved in Proposition 1 that the parameters have to verify the following constraint:

$$w_{\text{sgn}} d = O(n_{\text{sgn}}).$$

Now the parameter w_{sgn} can not be too small either, since for fixed w_{sgn} the algorithms for decoding linear codes also solve the signature forgery in polynomial time. This problem amounts in the case of the IBE to find a $\mathbf{u}_{id}$ such that

$$|\mathbf{u}_{id} \mathbf{G}_{\mathscr{C}_{\text{sgn}}} - \mathscr{H}(id)| = w_{\text{sgn}}.$$

We will therefore make a minimal assumption that ensures that the decoding algorithms for solving this problem have at least some (small) subexponential complexity. We also make the same assumption for the aforementioned recovery of $\mathbf{e}$. This is obtained by assuming that

Assumption 3.

$$d = \Omega(n^{\varepsilon}) \quad \textit{for some} \quad \varepsilon > 0 \tag{25}$$

$$w_{\text{sgn}} = \Omega(n^{\varepsilon'}) \quad \textit{for some} \quad \varepsilon' > 0 \tag{26}$$

Proposition 8. *Under Assumption 3, the Prange algorithm breaks the IBE scheme in Hamming metric in polynomial time in* $n_{\rm sgn}$.

Proof. Recall that parameters of the IBE in Hamming metric are $n_{\rm sgn}, k_{\rm sgn}, w_{\rm sgn}$. For the sake of simplicity let,

$$n \stackrel{\triangle}{=} n_{\rm sgn} \quad ; \quad k \stackrel{\triangle}{=} k_{\rm sgn} \quad ; \quad w \stackrel{\triangle}{=} w_{\rm sgn}.$$

We start the proof by noticing that $wd = O(n)$ and Assumption 3 actually imply the "converse" inequalities

$$\begin{aligned} d &= O(n^{1-\varepsilon'}) \\ w_{\rm sgn} &= O(n^{1-\varepsilon}) \end{aligned}$$

Let us now derive an asymptotic expression for (24) by studying:

$$\log_2 \binom{n}{d} - \log_2 \binom{k}{d}$$

This is obtained through:

Lemma 9.

$$\log_2 \binom{n}{l} = nh\left(\frac{l}{n}\right) + O\left(\log_2 n\right)$$

for h *being defined over* $[0,1]$ *as:*

$$h(x) \stackrel{\triangle}{=} -x \log_2 x - (1-x) \log_2 x$$

Therefore to show that the Prange algorithm is polynomial in n it is sufficient to prove that:

$$nh\left(\frac{d}{n}\right) - kh\left(\frac{d}{k}\right) \tag{27}$$

is an $O\left(\log_2 n\right)$. Recall now that in a context of code-based hash and sign, the weight of the decoding has to be greater than the Varshamov Gilbert bound, namely:

$$w \geq nh^{-1}\left(1 - \frac{k}{n}\right) \iff \frac{k}{n} \geq 1 - h\left(\frac{w}{n}\right)$$

From $w = O\left(n^{1-\varepsilon}\right)$, $k \leq n$ and by using that $h(x) \underset{x \to 0}{=} O\left(-x \log_2 x\right)$ we get:

$$\frac{k}{n} = 1 + O\left(-\frac{w}{n} \log_2 \frac{w}{n}\right) \tag{28}$$

and $k \sim n$. We are now ready to show that (27) is asymptotically an $O(\log_2 n)$. As $k \sim n$ and $d = O(n^{1-\varepsilon'})$ by using now that $h(x) \underset{x \to 0}{=} -x \log_2 x + \frac{1}{\ln(2)}\left(x - \sum_{l=2}^{p-1} \frac{x^l}{l(l-1)} + O(x^p)\right)$ for an integer p greater than $\frac{1}{\varepsilon'}$ we have:

$$nh\left(\frac{d}{n}\right) - kh\left(\frac{d}{k}\right) = a(n) + b(n) + c(n) \tag{29}$$

where

$$a(n) \stackrel{\triangle}{=} k\frac{d}{k} \log_2 \frac{d}{k} - n\frac{d}{n} \log_2 \frac{d}{n}$$

$$b(n) \stackrel{\triangle}{=} n\frac{d}{\ln(2)n} - k\frac{d}{\ln(2)k} + \frac{1}{\ln(2)} \sum_{l=2}^{p-1} k\frac{(d/k)^l}{l(l-1)} - n\frac{(d/n)^l}{l(l-1)} \tag{30}$$

and

$$c(n) \triangleq nO\left(\frac{d^p}{n^p}\right) + kO\left(\frac{d^p}{k^p}\right)$$

We easily have:

$$\begin{aligned} c(n) &= O\left(\frac{d^p}{n^{p-1}}\right) \\ &= O\left(\frac{1}{n^{p\varepsilon'-1}}\right) \quad \text{(because } d = O(n^{1-\varepsilon'})\text{)} \\ &= o(1) \quad \text{(because } p > 1/\varepsilon'\text{)} \end{aligned}$$

Let us now compute $a(n)$:

$$\begin{aligned} a(n) &= k\frac{d}{k}\log_2\frac{d}{k} - n\frac{d}{n}\log_2\frac{d}{n} \\ &= d\log_2\frac{d}{k} - d\log_2\frac{d}{n} \\ &= -d\log_2\frac{k}{n} \\ &= -d\log_2\left(1 + O\left(\frac{w}{n}\log_2\frac{w}{n}\right)\right) \quad \text{(because of (28))} \end{aligned}$$

Recall now that we have $w = O(n^{1-\varepsilon})$ and by using $\log_2(1+x) \underset{x\to 0}{=} O(x)$ we get:

$$a(n) = -dO\left(\frac{w}{n}\log_2\frac{w}{n}\right)$$

which gives as $wd = O(n)$ and $w = O(n^{1-\varepsilon})$:

$$a(n) = O\left(\log_2\frac{w}{n}\right) = O\left(\log_2 n\right) \tag{31}$$

Let us now compute $b(n)$ which is defined in (30):

$$\begin{aligned} b(n) &= n\frac{d}{\ln(2)n} - k\frac{d}{\ln(2)k} + \frac{1}{\ln(2)}\sum_{l=2}^{p-1} k\frac{(d/k)^l}{l(l-1)} - n\frac{(d/n)^l}{l(l-1)} \\ &= \frac{1}{\ln(2)}\sum_{l=2}^{p-1} d^l\frac{1}{n^{l-1}}\frac{(k/n)^{1-l}-1}{l(l-1)} \end{aligned}$$

Recall now that

$$\frac{k}{n} = 1 + O\left(-\frac{w}{n}\log_2\frac{w}{n}\right)$$

therefore,

$$\begin{aligned} \left(\frac{k}{n}\right)^{1-l} - 1 &= \left(1 + O\left(-\frac{w}{n}\log_2\frac{w}{n}\right)\right)^{1-l} - 1 \\ &= 1 + O\left(-\frac{w}{n}\log_2\frac{w}{n}\right) - 1 \\ &= O\left(-\frac{w}{n}\log_2\frac{w}{n}\right) \end{aligned}$$

Then we get:

$$\begin{aligned}
b(n) &= \frac{1}{\ln(2)} \sum_{l=2}^{p-1} \frac{d^l}{n^{l-1}} \frac{1}{l(l-1)} O\left(-\frac{w}{n} \log_2 \frac{w}{n}\right) \\
&= \frac{1}{\ln(2)} \sum_{l=2}^{p-1} \frac{d^{l-1}}{l(l-1)n^{l-1}} O\left(-\frac{dw}{n} \log_2 \frac{w}{n}\right) \\
&= \frac{1}{\ln(2)} \sum_{l=2}^{p-1} o(1) O\left(-\log_2 \frac{w}{n}\right) \\
&\qquad \text{(because } d = O(n^{1-\varepsilon'}) = o(n) \text{ as } \varepsilon' > 0 \text{ and } dw = O(n)\text{)}. \\
&= o\left(-\log_2 \frac{w}{n}\right) \\
&= O\left(\log_2 n\right)
\end{aligned}$$

Therefore, by combining this result with (29) and (31) we get:

$$kh\left(\frac{d}{k}\right) - nh\left(\frac{d}{n}\right) = O\left(\log_2 n\right)$$

which concludes the proof.

□

8 Concluding remarks

We have presented here our attacks against the rank-based signature scheme RankSign and the IBE scheme proposed in [GHPT17]. Several comments can be made.

Attack on RankSign. We actually showed that in the case of RankSign, the complexity is polynomial for all possible strategies for choosing the parameters. Repairing the RankSign scheme seems to require to modify the scheme itself, not just adjust the parameters. It might be tempting to conjecture that the approach against RankSign could also be used to mount an attack on the NIST submissions based on LRPC codes such as [ABD+17a, ABD+17b]. Roughly speaking our approach consists in looking for low weight codewords in the LRPC code instead of looking for low weight codewords in the usual suspect, that is the dual of the LRPC code, that has in this case low weight codewords by definition of the LRPC code. This approach does not seem to carry over to the LRPC codes considered in those submissions. The point is that our approach was successful for RankSign because of the way the parameters of the LRPC code had to be chosen. In particular the length n, the dimension k and the weight of the LRPC code have to satisfy

$$n = (n-k)d.$$

It is precisely this equality that is responsible for the weight 2 codewords in the LRPC code. If d is not too small (say > 3) and $(n-k)d$ is sufficiently above n, then the whole approach considered here fails at the very beginning.

Attack on the IBE [GHPT17]. The attack on RankSign also breaks the IBE proposal of [GHPT17] since it is based partly on the RankSign primitive. We have shown here that the problem is actually deeper than this by showing that even if a secure signature scheme replaces in the IBE, RankSign, then an attack that breaks directly the RSL problem which is the other problem on which the IBE is based, can be mounted for the parameters proposed in [GHPT17]. Again, as in the case of RankSign, the reason why this attack was successful comes from the fact that the constraints on the parameters that are necessary for the scheme to work properly work

in favor of ensuring that a certain code that can be computed from the public data has low weight codewords. These low codewords are then found by an algebraic attack. However, contrarily to the RankSign case, where the conditions on the parameters force a certain code to have codewords of low weight, this phenomenon can be avoided by a very careful choice of the parameters in the IBE. This opens the way for repairing the scheme of [GHPT17] if a secure signature scheme is found for the rank metric.

We have also studied whether the [GHPT17] approach for obtaining an IBE scheme based on coding assumptions could work in the Hamming metric. However in this case, and contrarily to what happens in the rank metric, we have given a devastating polynomial attack in the Hamming metric relying on using the simplest generic decoding algorithm [Pra62] that can not be avoided by any reasonable choice of parameters. It seems that following the GPV [GPV08]/[GHPT17] approach for obtaining an IBE scheme is a dead end in the case of the Hamming metric.

To conclude this discussion on [GHPT17], we would like to stress that our result in the Hamming case does not imply the impossibility of designing an IBE based on coding theory. It only suggests to investigate other paradigms rather than trying to adapt the GPV strategy. For instance, the recent progress of [DG17b, DG17a, DGHM18] made on the design of IBE's, particularly with the concept of one-time signatures with encryption, might be applied to cryptography based on decoding assumptions.

References

[ABD+17a] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. LAKE– Low rAnk parity check codes Key Exchange —-. first round submission to the NIST post-quantum cryptography call, November 2017.

[ABD+17b] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. LOCKER–LOw rank parity ChecK codes EncRyption –. first round submission to the NIST post-quantum cryptography call, November 2017.

[AGH+17] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Oliver Ruatta, and Gilles Zémor. Ranksign -a signature proposal for the NIST's call-. first round submission to the NIST post-quantum cryptography call, November 2017. NIST Round 1 submission for Post-Quantum Cryptography.

[Ale11] Michael Alekhnovich. More on average case vs approximation complexity. *Computational Complexity*, 20(4):755–786, 2011.

[AMAB+17] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Rank quasi cyclic (RQC). first round submission to the NIST post-quantum cryptography call, November 2017.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In *Advances in Cryptology - CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, August 2001.

[BFS99] Jonathan F. Buss, Gudmund S. Frandsen, and Jeffrey O. Shallit. The computational complexity of some problems of linear algebra. *J. Comput. System Sci.*, 58(3):572–596, June 1999.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Smaller decoding exponents: ball-collision decoding. In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 743–760, 2011.

[BM17] Leif Both and Alexander May. Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{2/21n}$ and McEliece Security. In *WCC Workshop on Coding and Cryptography*, September 2017. To appear, see `https://www.google.fr/?gfe_rd=cr&ei=lEyVWcPPBuXU8gfAj5ygBg`.

[BMvT78] Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, 24(3):384–386, May 1978.

[CFS01] Nicolas Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 157–174, Gold Coast, Australia, 2001. Springer.

[Cou01] Nicolas Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 402–421, Gold Coast, Australia, 2001. Springer.

[DG17a] Nico Döttling and Sanjam Garg. From selective IBE to full IBE and selective HIBE. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, pages 372–408, 2017.

[DG17b] Nico Döttling and Sanjam Garg. Identity-based encryption from the Diffie-Hellman assumption. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017*, volume 10401 of *LNCS*, pages 537–569, Santa Barbara, CA, USA, August 2017. Springer.

[DGHM18] Nico Döttling, Sanjam Garg, Mohammad Hajiabadi, and Daniel Masny. New constructions of identity-based and key-dependent message secure encryption schemes. In Michel Abdalla and Ricardo Dahab, editors, *Public-Key Cryptography - PKC 2018*, volume 10769 of *LNCS*, pages 3–31, Rio de Janeiro, Brazil, March 2018. Springer.

[DT17] Thomas Debris-Alazard and Jean-Pierre Tillich. Statistical decoding. preprint, January 2017. arXiv:1701.07416.

[Dum91] Ilya Dumer. On minimum distance decoding of linear codes. In *Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory*, pages 50–52, Moscow, 1991.

[FDS10] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In *Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings*, pages 257–264, 2010.

[FLdVP08] Jean-Charles Faugère, Françoise Levy-dit Vehel, , and Ludovic Perret. Cryptanalysis of Minrank. In David Wagner, editor, *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *LNCS*, pages 280–296, 2008.

[FS09] Matthieu Finiasz and Nicolas Sendrier. Security bounds for the design of code-based cryptosystems. In M. Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 88–105. Springer, 2009.

[Gab08] Ernst. M. Gabidulin. Attacks and counter-attacks on the GPT public key cryptosystem. *Des. Codes Cryptogr.*, 48(2):171–177, 2008.

[GHPT17] Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich. Identity-based encryption from rank metric. In *Advances in Cryptology - CRYPTO2017*, volume 10403 of *LNCS*, pages 194–226, Santa Barbara, CA, USA, August 2017. Springer.

[GMRZ13] Philippe Gaborit, Gaétan Murat, Olivier Ruatta, and Gilles Zémor. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. Available on `www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf`.

[GO01] Ernst M. Gabidulin and Alexei V. Ourivski. Modified GPT PKC with right scrambler. *Electron. Notes Discrete Math.*, 6:168–177, 2001.

[GPT91] Ernst M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their applications to cryptography. In *Advances in Cryptology - EUROCRYPT'91*, number 547 in LNCS, pages 482–489, Brighton, April 1991.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.

[GRS13] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *CoRR*, abs/1301.1026, 2013.

[GRS16] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Information Theory*, 62(2):1006–1019, 2016.

[GRSZ14] Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor. Ranksign: An efficient signature algorithm based on the rank metric (extended version on arxiv). In *Post-Quantum Cryptography 2014*, volume 8772 of *LNCS*, pages 88–107. Springer, 2014.

[GZ16] Philippe Gaborit and Gilles Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Trans. Information Theory*, 62(12):7245–7252, 2016.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in Cryptology - CRYPTO'99*, volume 1666 of *LNCS*, pages 19–30, Santa Barbara, California, USA, August 1999. Springer.

[LB88] Pil J. Lee and Ernest F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In *Advances in Cryptology - EUROCRYPT'88*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

[Loi14] Pierre Loidreau. Asymptotic behaviour of codes in rank metric over finite fields. *Des. Codes Cryptogr.*, 71(1):105–118, 2014.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $O(2^{0.054n})$. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[MO15] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[Nie86] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology - CRYPTO 84*, volume 196 of *LNCS*, pages 47–53. Springer, 1984.

[SOK00] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing. In *SCIS 2000*, Okinawa, Japan, January 2000.

[Spa12] Pierre-Jean Spaenlenhauer. *Résolution de systèmes multi-homogènes et determinantiels*. PhD thesis, Univ. Pierre et Marie Curie- Paris 6, October 2012.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.